KEMAMPUAN HUKUM PIDANA TERHADAP KEJAHATAN SIBER TERKAIT PERLINDUNGAN DATA PRIBADI DI INDONESIA

TESIS

OLEH :

NAMA MHS : BAGUS SATRYO RAMADHA, S.H

NO. POKOK MHS : 18912046

BKU : HUKUM DAN SISTEM PERADILAN PIDANA

PROGRAM MAGISTER ILMU HUKUM

FAKULTAS HUKUM

UNIVERSITAS ISLAM INDONESIA

2021

KEMAMPUAN HUKUM PIDANA TERHADAP KEJAHATAN SIBER TERKAIT PERLINDUNGAN DATA PRIBADI DI INDONESIA

Oleh:

Nama Mahasiswa	:	BAGUS SATRYO RAMADHA, S.H
NIM	:	18912046
BKU	:	HUKUM DAN SISTEM PERADILAN PIDANA

Telah diperiksa dan disetujui oleh Dosen Pembimbing untuk diajukan kepada Tim Penguji dalam Ujian Akhir/Tesis
Program Studi Hukum Progtram Magister

Pembimbing

Dr. M. Arif Setiawan, S.H., M.H

Yogyakarta, 4 Maret 2021

Mengetahui
Ketua Program Studi Hukum Program Magister
Fakultas Hukum Universitas Islam Indonesia

Aunur Rohim Faqih, S.H., M.Hum., Ph.D.

KEMAMPUAN HUKUM PIDANA TERHADAP KEJAHATAN SIBER TERKAIT PERLINDUNGAN DATA PRIBADI DI INDONESIA

Oleh:

Nama Mahasiswa	:	BAGUS SATRYO RAMADHA, S.H
NIM	:	18912046
BKU	:	HUKUM DAN SISTEM PERADILAN PIDANA

Telah diujikan dihadapan Tim Penguji dalam Ujian Akhir/Tesis
dinyatakan LULUS

Pembimbing

Dr. M. Arif Setiawan, S.H., M.H. Yogyakarta, 25 Maret 2021
Anggota Penguji 1

Dr. Mahrus Ali, S.H., M.H. Yogyakarta, 25 Maret 2021
Anggota Penguji 2

Dr. Aroma Elmina Martha, S.H., M.H. Yogyakarta, 25 Maret 2021

Mengetahui
Ketua Program Studi Hukum Program Magister
Fakultas Hukum Universitas Islam Indonesia

Dr. Agus Triyanta, M.A., M.H., Ph.D.

SURAT PERNYATAAN

ORISINALITAS KARYA TULIS ILMIAH MAHASISWA

PROGRAM PASCASARJANA

FAKULTAS HUKUM UNIVERSITAS ISLAM INDONESIA

بسم الله الرحمن الرحيم

Yang bertandatangan di bawah ini, saya:

Nama : Bagus Satryo Ramadha, S.H

NIM : 18912046

BKU : Hukum dan Sistem Peradilan Pidana

Menyatakan telah melakukan penulisan Karya Tulis Ilmiah (Tugas Akhir) berupa Tesis dengan judul

"KEMAMPUAN HUKUM PIDANA TERHADAP KEJAHATAN SIBER TERKAIT PERLINDUNGAN DATA PRIBADI DI INDONESIA"

Karya ilmiah telah saya ajikan kepada Tim Penguji dalam sidang akhir yang diselenggarakan aoleh Program Pascasarjana Fakultas Hukum Magister Hukum Universitas Islam Indonesia. Schubungan dengan hal tersebut, dengan ini saya menyatakan:

1. Bahwa karya tulis ilmiah ini adalah benar-benar karya saya sendiri yang dalam penyusunannya tunduk dan patuh terhadap kaidah, etika dan norma-nomra penulisan sebuah karya tulis ilmiah sesuai dengan ketentuan yang berlaku;
2. Bahwa saya menjamin hasil karya ilmiah ini benar-benar asli (Orisinil), bebas dair unsur-unsur yang dapat dikategorikan sebagai melakukan perbuatan penjiplakan karya ilmiah (Plagiat);
3. Bahwa mesikpun secara prinsip hak milik atas karya ilmiah ini pada saya, namun demi untuk kepentingan yang bersifat akademik dan pengembangannya, saya memberikan kewenangan kepada perpustakaan Fakultas Hukum UII dan Perpustakaan di Lingkungan UII untuk mempergunakan karya ilmiah saya tersebut.

Selanjutnya berkaitan dengan hal di atas (terutama pernyataan pada butir No. 1 dan 2), saya sanggup menerima sanksi administrarif, akademik, dan sanksi pidana, jika saya terbukti secara sah dan meyakinkan telah melakukan perbuatan yang menyimpang dari pernyataan tersebut, saya juga akan bersifat kooperatif untuk hadir, menjawab membuktikan, melakukan pembelaan terhadap hak saya serta menandatangani berita acara terkait yang menjadi hak dan kewajiban saya, di depan "majelis" atau "TIM" Fakultas Hukum UII yang ditunjuk oleh Pimpinan Fakultas apabila tanda-tanda plagiat disinyalir ada atau terjadi pada karya ilmiah sata oleh pihak Fakultas Hukum UII.

Demikian surat pernyataan ini saya buat dengan sebenar-benarnya dan dalam kondisi sehat jasmani dan rohani, dengan sadar serta tidak ada tekanan dalam bentuk apapun dan oleh siapapun.

Yogyakarta, 25 Maret 2021

(Bagus Satryo Ramadha, S.H)

MOTTO

“Sebaik-baiknya manusia adalah yang paling bermanfaat untuk orang lain”

(**Sabda Nabi Muhammad SAW: H.R Bukhori)**

“Barang siapa keluar untuk mencari ilmu maka dia berada di jalan Allah”

(H.R Turmudzi)

“Allah mencintai pekerjaan yang apabila pekerjaanya diselesaikan dengan baik olehnya”

(H.R Thabrani)

PERSEMBAHAN

- Karya ini ku haturkan kehadirat Allah SWT yang Maha Esa dan memiliki Ilmu yang Maha Kekal
- Karya ini juga aku persembahkan kepada kedua orang tua Ayahanda tercinta Drs. Prasetyo, Bc, Ip, M.H dan Ibunda tercinta Tristiana Erni Sumartini yang selalu memberikan kasih sayang yang luar biasa
- Kepada Kakakku Bagas Galih Sasmito yang memberikan dorongan dan semangat

KATA PENGANTAR

Assalammualaikum Wr. Wb

Puji syukur penulis panjatkan kehadirat Tuhan Yang Maha Esa atas limpahan rahmat-Nya sehingga penulis dapat mengatasi segala rintangan dan kesulitan sampai akhirnya dapat menyelesaikan penulisan tesis sesuai dengan yang diharapkan. Adapun maksud dan tujuan penulisan tesis ini adalah untuk memenuhi sebagian syarat-syarat guna memperoleh gelar Magister (S-2) bagian Hukum Pidana pada Magister Ilmu Hukum Universitas Islam Indonesia Yogyakarta. Dalam penulisan tesis ini penulis tidak lupa mengucapkan terima kasih atas bantuan dan kerjasama dari berbagai pihak. Ucapan terima kasih ini penulis haturkan kepada:

1. Prof. Fathul Wahid, S.T., M.Sc., Ph.D. selaku Rektor Universitas Universitas Islam Indonesia Yogyakarta.
2. Dr. Abdul Jamil, S.H., M.H. selaku Dekan Fakultas Hukum Universitas Universitas Islam Indonesia Yogyakarta.
3. Drs. Agus Triyana, M.H., MA., Ph.D., selaku Ketua Program Studi Magister Ilmu Hukum Fakultas Hukum Universitas Universitas Islam Indonesia Yogyakarta.
4. Dr. M. Arif Setiawan, S.H., M.H. selaku Dosen Pembimbing yang telah banyak memberikan pengarahan dan petunjuk serta mencurahkan segala waktu yang sangat berguna dalam penulisan hukum.
5. Bapak dan Ibu Dosen beserta seluruh Staf Fakultas Hukum Universitas Islam Indonesia Yogyakarta.

6. Kedua orang tua saya Drs. Prasetyo, Bc. Ip, M.H dan Tristiana Erni Sumartini S.H tercinta beserta seluruh keluarga yang telah memberikan dukungan moril dan materiil.
7. Kakakku Bagas Galih Sasmito yang selalu mendukung dalam hal menuntut ilmu.
8. Nita Praningsih S.H yang telah memberikan dukungan dan semangat untuk menyelesaikan hingga tahap ini.
9. Seluruh keluarga Kos Arjuna YK yang selalu memberikan motivasi dan inspirasi
10. Seluruh rekan-rekan di Magister Ilmu Hukum Angkatan 42 Universitas Islam Indonesia dan semua pihak yang tidak dapat disebutkan satu-persatu.

Semoga amal dan kebaikan saudara-saudara mendapatkan pahala dari Tuhan Yang Maha Esa. Penulis menyadari segala kekurangan dan ketidaksempurnaan penulisan tesis ini, dengan segala kerendahan hati penulis dengan senang hati menerima kritik dan saran yang sifatnya membangun guna perbaikan dan kesempurnaan penulisan tesis ini..

Yogyakarta, 25 Maret 2021

(Bagus Satryo Ramadha, S.H)

DAFTAR ISI

KEMAMPUAN HUKUM PIDANA TERHADAP KEJAHATAN SIBER TERKAIT PERLINDUNGAN DATA PRIBADI DI INDONESIA

ABSTRAK

Studi ini bertujuan untuk mengetahui bagaimana kemampuan hukum pidana di Indonesia mengenai kejahatan siber terkait perlindungan data pribadi dan kendala apa saja yang menjadi faktor dalam menanggulangi kejahatan siber terkait perlindungan data pribadi. Tujuan penelitian ini fokus yaitu kemampuan hukum pidana terhadap kejahatan siber terkait perlindungan data pribadi dan faktor yang menjadi kendala dalam menanggulangi kejahatan siber terkait perlindungan data pribadi di Indonesia. Pendekatan yang digunakan dalam penelitian ini adalah pendekatan normatif, yaitu metode penelitian hukum yang mengkaji hukum tertulis dan kepustakaan atau penelitian hukum dari beragam perspektif, bahan hukum yang digunakan ialah bahan hukum primer dan bahan hukum sekunder. Analisis dilakukan secara deskriptif yaitu mengumpulkan semua data dan menghubungkan permasalahan dengan analisis berdasarkan teori hukum yang disusun sistematis.

Hasil penelitian ini menunjukan bahwa data pribadi yang bersifat elektronik termasuk dalam informasi elektronik yang dilindungi. UU ITE mengenal Sistem keamanan yang memberikan perlindungan terhadap data atau informasi terhadap akses illegal dengan adanya kode akses atau password serta adanya gangguan data yang juga dikenal dalam UU ITE. Kendala atas perlindungan data pribadi kurangnya pengaturan dalam UU ITE untuk menjangkau akan klasifikasi data yang dilindungi sebagai bentuk untuk memberikan kejelasan akan data yang dapat diakses.

Kata Kunci: Kejahatan Siber, Perlindungan Data, Data Pribadi

ABSTRACT

The study aims to find out how law enforcement form in Indonesia about cybercrime related to personal data protection and what challenges law enforcement can make agaianst cybercrime. The perpose of this study is the focus of law enforcement of cybercrime in Indonesia. The approach used in this study is the normative approach, which is the method of law study which examines written law and literature or legal research from various perspectives, the leal material used is primary and secondary legal material. A descriptive analysis used to collect all the data and connect the problem with an analysis of legal theory.

This study has shown that recognizes security systems that provide protection against data or information against illegal access with access code or passwords. The personal data proction problem is the lack of setting in the bill for reaching out to select protected data classification as forms to bring clarity to the accessible data.

Keywords: Cybercrime, Data Protection, Personal Data

BAB I

PENDAHULUAN

A. Latar Belakang

Globalisasi dipandang dan dipahami sebagai proses lazim yang tidak dapat dihindari dari semakin majunya peradaban manusia di bidang ilmu pengetahuan dan teknologi (Iptek), khususnya terhadap teknologi komunikasi dan informasi,[1] dengan kemajuan teknologi yang begitu pesat, penggunaan media elektronik dan teknologi informasi mempunyai peranan yang signifikan dan telah merambah pada berbagai sektor kehidupan manusia. Posisi media elektronik dan teknologi informasi juga merubah pada tataran kehidupan masyarakat sehari-hari dipandang dari sisi ekonomi, hukum, politik dan budaya. Sehingga teknologi tidak lagi bisa dianggap sebelah mata dalam penggunananya.

Penggunaan teknologi sistem informasi dan teknologi informasi dimulai pada inovasi teknologi sistem informasi yang berbasis pada integrasi antara teknologi komunikasi dengan teknologi komputer, atau disebut *interconnection networking* yang dikenal sebagai **"Internet"**, bisa juga dimaknai sebagai *global networking of computer networks* atau sebuah jaringan komputer dalam skala universal.[2] Aktifitas penggunaan teknologi tidak sesederhana lagi karena kegiatannya tidak dibatasi oleh

[1] Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (Cybercrime)*, Cetakan kedua (Bandung: Refika Aditama, 2010), hlm 6.

[2] Jack Febrian, *Menggunakan Internet,* (Bandung: Informatika, 2003), hlm 3.

territorial suatu negara *(borderless)*, yang dapat diakses dengan mudah.[3] Kerugian yang berdampak dapat terjadi dari berbagai aspek dan bahkan bisa berimbas langsung terhadap perorangan, masyarakat dan bahkan di suatu negara tertentu. Hal ini berujung pada implikasi munculnya suatu pasar baru yang mendorong perkembangan dalam sistem ekonomi masyarakat, awalnya berbasis ekonomi konvensional yang mengarah pada *digital economy* yang berpangkal pada informasi, kreativitas intelektual dan ilmu pengetahuam yang sering dikenal dengan *creative economy.*[4]

Keuntungan penggunaan Internet dalam berbagai bidang menjadi lebih mudah, tetapi disisi lain tentu menimbulkan keadaan baru yang harus diperhatikan sebagai pengaturan agar lebih menjamin penggunaan bagi pengguna di internet terlindungi atas perlindungan data pribadinya *(the protection of privacy rights)* dan terhindar dari penyalahgunaan yang berdampak dapat menimbulkan kerugian terhadap masyarakat sosial. Pentingnya perlindungan terhadap akses data pribadi pengguna dari kejahatan siber menjadi pertimbangan serius ditambah meningkatnya jumlah pengguna telepon seluler dan internet belakangan ini,[5] serta tak ada jaminan yang pasti atas data pribadi dapat terhindar dari kejahatan siber.

---

[3] Widodo, *Aspek Hukum Pidana Kejahatan Mayantara,* Cetakan pertama, (Yogyakarta: Aswaja, 2013), hlm 17.

[4] Edmon Makarim, *Tanggung Jawab Hukum Penyelenggara Sistem Elektronik,* (Jakarta: Raja Grafindo Persada, 2010), hlm 2.

[5] Wahyudi Djafar dan Asep Komarudin, *Perlindungan Hak Atas Privasi Di Internet: Beberapa Penjelasan Kunci,* terbitan pertama, (Jakarta: ELSAM, 2014), hlm 1.

Data dari hasil Norton Report 2013 memperlihatkan indikasi dan akibat terhadap tindak kejahatan siber di Indonesia cukup serius dan adanya peningkatan yang dilansir di laman Id-SIRTAII/CC *(Indonesia Security Incedent Response Team on Internet Infrastructure/Cordination Center)*.[6] Hasil survey yang juga dilakukan Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) dari data tiga tahun terakhir dimulai dari tahun 2016-2018 terus mengalami peningkatan, terlihat pada tahun 2016 pengguna jasa Internet 132,7 juta atau setara 51,7% terhadap populasi 256,2 juta jiwa, pada tahun berikutnya 2017 meningkat 143,26 juta pengguna atau setara 54,68% dari populasi penduduk 262 juta jiwa, dan tahun 2018 pengguna jasa internet sudah mencapai 171,17 juta pengguna atau naik 10,12% dari tahun lalu dari populasi saat ini 254,16 juta jiwa.[7] Sedangkan laporan dari riset yang dilakukan oleh "*we are social"* menunjukan peningkatan penggunaan internet pada tahun 2019-2020 per-januari dengan persentase kenaikan 17% dari tahun sebelumnya atau penambahan 25 juta pengguna dengan skala populasi penduduk 272.,1 juta. [8] Data tersebut memberikan gambaran bahwa seiring dengan pesatnya peningkatan pengguna internet, masyarakat juga mulai menyadari resiko penyalahgunaan data pribadinya dari mengunjungi setiap situs atau aplikasi online tertentu dengan mengisi identittas pribadi yang diperlukan sebagai syarat akun di situs-situs tertentu

[6] Rosalinda Elsina Latumahina, *Aspek Hukum Perlindungan Data Pribadi di Dunia Maya*, Jurnal Gema Aktualita, Edisi No. 2, Vol. 3, Desember 2014, hlm 15.

[7] Tim APJII, "Penetrasi dan Profil Perilaku Pengguna Internet Indoensia", *Buletin Asosiasi Penyelenggara Jasa internet Indonesia (APJII),* Edisi 40 Mei 2020, hlm 1-2.

[8] https://andi.link/hootsuite-we-are-social-indonesian-digital-report-2020/, hlm 24, diakes 8 Oktober 2020.

dengan tujuan untuk mempermudah mencari keinginan dari penggunanya. Sehingga tidak dapat dihindari lagi akan situs-situs yang wajib mencantumkan data pribadi dalam akun tersebut menjadi rentan akan hal yang dapat merugikan pemilik data dari akunnya.

Kekhawatiran penyalahgunaan atas data pribadi juga terlihat bahwa presentase sebanyak 59% pengguna internet merasa cemas bila data pribadinya disalah gunakan oleh perusahaan atau pihak-pihak tertentu dengan motif keuntungan semata yang berimbas merugikan pemilik data.[9] Peningkatan pengguna internet tidak terlepas dari kesadaran masyarakat terhadap teknologi yang menuntut atas kemudahan di era globalisasi sebagai faktor pendukung terhadap aktifitas lainnya termasuk timbulnya bentuk kejahatan-kejahatan baru.

Data pribadi di era abad ke 21 ini menjadi "barang seksi", sebab peralihan di dunia nyata yang kian bergeser ke hal yang baru berbentuk serba visual menjadi hal yang kian mudah segala aktivitas dilakukan. Adagium "kejahatan merupakan produk dari masyarakat itu sendiri" berlaku terhadap pesatnya perkembangan teknologi informasi yang menimbulkan hal baru di dunia hukum. Kriminalitas penggunaan teknologi sebagai media yang berbasis internet muncul dan semakin berkembang di masyarakat yang menjadikan hal biasa.[10]

[9] Ibid, hlm 32.

[10] Afitrahim, *Yurisdiksi Dan Transfer of Proceeding Dalam Kasusu Cybercrime,* Tesis, Universitas Indonesia, 2012, hlm 2.

Suatu masyarakat hukum memiliki nilai-nilai yang dianut bersama atau berkenaan dengan penghargaan kolektif (*sinngebungen)* atau kepentingan hukum tentang apa yang baik, benar dan karena itu patut diraih. Nilai-nilai dimaksudkan untuk melindungi, baik terhadap pelanggaran maupun ancaman bahaya (resiko), dengan cara memuruskan suatu ketentuan pidana.[11] Negara seharusnya memberikan keamanan terhadap data pribadi bagi masyarakat yang berpotensi baik dalam bentuk penyalahgunaan atau kejahatan yang berasal dari dalam maupun luar negara. Sehingga negara dianggap perlu untuk memiliki regulasi yang menggambarkan dan memetakan klasifikasi bahwa data pribadi dibatasi dalam keadaan tertentu dan langkah-langkah yang diambil dengan dasar keputusan yang khusus oleh otoritas negara sebagai perlindungan dan jaminan oleh hukum atas pelanggaran yang merugikan.

Regulasi yang mengatur berkaitan perlindungan data pribadi di Indonesia memang secara eksplisit telah diatur di beberapa Undang-Undang, semisal Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan, Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan, Undang-Undang Nomor 24 tahun 2013 tentang Administrasi Kependudukan, dan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Pada Pasal 26 Ayat (1) Undang-Undang ITE mengenai informasi melalui media elektronik yang mengandung data pribadi tidak menjelaskan secara

[11] J. Remmelink, *Pengantar Hukum Pidana Material; Prolegomena dan Uraian Tentang Teori-Ajaran Dasar,* Tristam P. Moeliono (penerjemah), (Yogyakarta: Maharsa, 2014), hlm 13.

detail dan kompherensif mengenai prinsip-prinsip perlindungan data pribadi, hak dan kewajiban bagi pemilik data dan *stakeholder* atau pemerintah dalam mengolah dan menggunakan data pribadi. Penjelasan Undang-Undang pada Pasal tersebut hanya memberikan definisi secara umum mengenai hak pribadi. Pada Ayat (2) dapat dilihat konseksuensi bila terjadi pelanggaran berkaitan dengan data pribadi yang hanya bersifat ganti rugi, potensi lemahnya kedudukan pemilik dari data pribadi terlihat ketika terjadi suatu tindakan yang merugikan pemilik data pribadi, bahkan pemilik data pribadi tidak menyadari telah dirugikan dan dalam hal ini peran negara hanyalah bersifat pasif. Konstitusi telah mengatur mengenai hak setiap orang atas perlindungan diri pribadi, walaupun tidak secara detail mencantumkan mengenai perlindungan data pribadi. Regulasi tersebut juga diikuti dengan kebijakan pemerintah yang mereformasi birokrasi secara masif dengan mulai beralih menggunakan media elektronik/digital.

Dua metode yang dikenal untuk memberikan perlindungan atas data pribadi yakni, *pertama* pengamanan terhadap data pribadi bersifat fisik, *kedua*, dilakukannya perlindungan data pribadi melalui regulasi dengan tujuan memberikan jaminan terhadap pengguna data pribadi,[12] maupun pihak pengelola *(provider)* atas potensi pelanggaran yang dilakukan di dunia *cyber*space yang basisnya menggunakan data pribadi sebagai aset komoditi yang menguntungkan.

[12] Wahyudi Djafar, Bernhard Ruben, dan Blandina, *Perlindungan data pribadi: Usulan Pelembagaan Kebijakan dari Perspektif Hak Asasi Manusia*, publis pertama, (Jakarta: Lembaga Studi dan Advokasi Masyarakat (ELSAM), 2016), hlm 4.

Secara umum data pribadi dapat diklasifikasikan menjadi dua, yaitu berkaitan dengan identitas personal dan yang berkolerasi dengan informasi pengguna.[13] Identitas personal sendiri menggambarkan subyek/orang secara kompherensif yang terdapat informasi yang secara mutlak hak dari subyek tersebut, sedangkan korelasi informasi pengguna di ruang siber bisa berupa data yang dapat memberikan dukungan yang berisfat keuntungan sosial, ekonomi dan politik.

Timbulnya masalah hukum mengenai penjelasan diatas terhadap kejahatan tindak pidana siber maka penulis tertarik untuk mengangkat judul "**Kemampuan Hukum Pidana Terhadap Kejahatan Siber Terkait Perlindungan Data Pribadi Di Indonesia".**

B. Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan sebelumnya, maka rumusan masalah agar mempermudah pembahasan selanjutnya. Adapun yang akan dikemukakan adalah sebagai berikut:

1. Bagaimana kemampuan pidana pada Undang-Undang Informasi dan Transaksi Elektronik dalam menanggulangi kejahatan siber terkait perlindungan data pribadi ?

[13] Wahyudi Djafar, *Perlindungan Hak Atas Privasi Di Internet, Beberapa Penjelasan Kunci,* publikasi pertama, (Jakarta: Lembaga Studi dan Advokasi Masyarakat (ELSAM), 2014), hlm 3.

2. Apa yang menjadi kendala pada Undang-Undang Informasi dan Transaksi Elektronik dalam menanggulangi tindak pidana kejahatan siber terkait perlindungan data pribadi di Indonesia ?

C. Tujuan Penelitian

Adapun tujuan penelitian ini adalah sebagai berikut:

1. Untuk mengetahui bagaimana kemampuan hukum pidana pada Undang-Undang Informasi dan Transaksi Elektronik dalam menanggulangi kejahatan siber terkait perlindungan data pribadi
2. Untuk mengetahui apa yang menjadi kendala pada Undang-Undang Informasi dan Transaksi Elektronik dalam menanggulangi tindak pidana kejahatan siber terkait perlindungan data pribadi di Indonesia.

D. Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan kontribusi yang positif yaitu:

1. Kegunaan Praktis

   Kegunaan praktis yang dimaksud merupakan keseluruhan data dan informasi yang disajikan dalam bentuk laporan hasil penelitian ini, diharapkan dapat memberikan atau menjadi literatur dalam praktek penegakan hukum terhadap kejahatan siber di ruang siber.

2. Kegunaan Teoritis

   Selesainya tesis ini diharapkan dapat memberikan kontribusi pemikiran untuk peningkatan dan pengembangan serta pembaharuan ilmu hukum pidana sesuai dengan tuntunan dan perkembangan zaman, khususnya dalam konteks

perkembangan teknologi, informasi elektronik, dan komunikasi berbasis teknologi.

E. Orisinalitas

Berdasarkan hasil penelusuran kepustakaan yang telah dilakukan, penulis menemukan hasil penelitian yang telah dipublikasikan yang di dalamnya tidak terdapat kesamaan. Menurut pengamatan penulis hasil tersebut akan dijadikan sebagai bahan pertimbangan dan acuan dalam melaksanakan penelitian hukum yang mendekati dengan penelitian yang dilakukan penulis, sebagai berikut:

Tabel 1: Beberapa Hasil Penelitian Terdahulu

No.	Judul/Nama/Bentuk/Tahun	Hasil Penelitian	Perbedaan
1.	Kebijakan Penanggulangan Tindak Pidana Teknologi Informasi melalui Hukum Pidana, Philemon Ginting, Tesis, 2008.[14]	Kebijakan formulasi hukum pidana terhadap tindak pidana teknologi informasi saat ini sebelum diundangkan Undag-Undang ITE terdapat beberapa ketentuan perundangan-undangan yang berhubungan dengan penanggulangan tindak pidana teknologi informasi, tetapi kebijakan formulasinya berbeda-beda terutama terkait kebijakan kriminalisasinya yang	Perbedaan dengan penelitian sebelumnya adalah objek penelitian yang akan dibahas dan waktu penelitiannya. Perbedaan dengan penelitian sebelumnya, tidak membahas mengenai kemampuan hukum pidana terkait tindak pidana terhadap kejahatan siber terkait

[14] Philemon Ginting, *Kebijakan Penanggulangan Tindak Pidana Teknologi Informasi Melalui Hukum Pidana,* Tesis, Magister Hukum, Program Studi Magister Hukum, Universitas Diponegoro, 2008.

		belum mengatur secara tegas dan jelas, kebijakan formulasi dalam Undang-Undang ITE masih dibutuhkan harmonisasi/singkronisasi baik secara internal maupun eksternal terutama instrument hukum insternasional terkait teknologi informasi.	perlindungan data pribadi.
2.	Perlindungan Hukum terhadap Pengguna *Cloud Computing* Atas Privasi dan Data Pribadi, Muh. Firmansyah Pradana, Tesis, 2018.[15]	Pengaturan pada Undang-Undang ITE sangat tidak signifikan dalam mengatur penggunaan data pribadi sebab hanya berupa ketentuan umum dan tidak menjelaskan berbagai isu yang banyak diperbincangkan, dalam Undang-Undang tersebut juga tidak dijelakan maksud dari proses pengumpulan, pemrosesan, penyimpanan, dan sejenisnya	Kajian yang dilakukan oleh peneliti sebelumnya mengenai perlindungan privasi dan data pribadi pada penggunaan *Cloud Computing*, yang membedakan dengan peneliti ialah objek penelitiannya dan sejauh mana hukum pidana pada Undang-Undang ITE dapat menjangkau

[15] Muh. Firmansyah Pradana, *Perlindungan Hukum Terhadap Pengguna Cloud Computing atas Perivasi dan Data Pribadi*, Tesis, Magister Hukum, Program Magister Hukum, Universitas Hasanuddin, 2018.

			terhadap tindak pidana siber terkait perlindungan data pribadi.
3.	Analisis Yuridis Perlindungan Data Yang Diperoleh Dari Pengguna Closed Circuit Television (CCTV) Yang Terhubung Dengan Teknologi Pengenal Wajah (Face Recognition) Di Ruang Publik, Noerdin Dinah Rasjidin, Tesis, 2020[16]	Pengaturan mengenai perlindungan hukum terhadap pengunaan CCTV di Indonesia belum ada regulasinya. Penggunaan CCTV yang menggunakan teknologi pengenal wajah pada tataran regulasinya masih terdapat tumpeng tindih dan kekosongan hukum terhadap transparansi, privasi, dan penyadapan, serta upaya hukum yang dilakuka terkait penggunaan CCTV di ruang publik, serta tidak adanya penyelesaian bahkan aduan serta proses mengajukan gugatan ke Pengadilan	Peneliti membedakan dengan penelitian sebelumnya terkait dengan perlindungan hukum terhadap privasi dan data pribadi dalam penggunaan CCTV, sedangkan yang akan diteliti penulis kemampuan Undang-Undang ITE dalam memberikan menanggulangi tindak pidana siber terkait perlindungan data pribadi..

[16] Noerdin Dinah Rasjidin, *Analisis Yuridis Perlindngan Data Yang Diperoleh Dari Pengguna Closed Circuit Television (CCTV) Yang Terhubung Dengan Teknologi Pengenalan Wajah (Face Recognition) Di Ruang Publik,* Tesis, Magister Hukum, Program Pascasarjana, Universitas Pelita Harapan, 2020.

F. Landasan Teori dan Doktrin

1. Kejahatan Siber

   a. Konsep Kejahatan Siber *(cyber crime)*

   Penggunaan terminologi siber *(cyber)* sering dikaitakan dengan sistem informasi, jaringan, komputer dan yang berhubungan dengan internet, penggunaan istilah tersebut sebenarnya memiliki interpretasi yang luas dan belum ada secara baku mengenai definisi tersebut. Penggunaan penulisan dari istilah siber pun dapat berupa kata benda atau sebagai kata sifat. Beberapa negara dan organisasi mendefinisikan istilah tersebut menurut pengertiannya masing-masing. Setidaknya penggunaan istilah siber *(cyber)* terdapat 26 definisi dibeberapa literature berkatian dengan dokumen-dokumen strategis keamanan dibeberapa negara. Namun pengertian siber *(cyber)* merujuk pada hal-hal sebagai berikut:[17]

   1) Infrasturktur fisik: erat kaitannya dengan infrastruktur kritis informasi
   2) Jaringan Komunikasi: mengacu pada komunikasi dan jaringan internet
   3) Sistem: erat hubungannya dengan sistem informasi di bidang bisnis, sistem infrastruktur, dan jasa
   4) Perangkat/piranti: mengarah pada perangkat keras seperti komputer, server, router, yang terkoneksi dengan internet
   5) Dunia maya: dunia digital yang berkaitan pada yurisdiksi negara.

[17] Riza Azmi. "Sejarah dan Konteks Terminologi Siber" *Majalah Cyber Defense Community*, edisi pertama tahun 2020, hlm 26-29.

Sehingga istilah siber saat ini lebih digunakan untuk mengacu pada infrastruktur fisik, komunikasi/jaringan komputer, sistem informasi, dan di dunia maya yang di dalamnya termasuk asset informasi dan non-informasi seperti individu, organisasi, pemerintahan, masyarakat, perangkat keras dan piranti yang dapat berinteraksi satu sama lain secara luas.

Kejahatan siber menjadi salah satu bentuk dimensi baru dari kejahatan saat ini yang menimbulkan perhatian dunia internasional. Berbagai istilah muncul seperti pendapat Volodymyr Golubev dalam buku Barda Nawani sebagai "*the new form of anti-social behavior"*, perkembangan dari kejahatan tersebut memunculkan istilah yang semakin dikenal sebagai kejahatan dunia maya *(cyber-space/virtual-space offence)* dimensi baru dari *"hi-tech crime"*. ITAC *(Information techonology association of Canada)* menjelaskan bahwa *"cybercrime is a real and growing threat to ecomonic and social development around the world. Information technology touches every aspect of human life and so can electronically enable crime"*,[18] terjemahan bebas bahwa kejahatan siber merupakan kejahatan yang nyata dan ancaman terhadap ekonomi dan perkembangan sosial di dunia. Teknologi informasi menyentuh pada berbagai aspek dari kehidupan manusia dan bisa menjadikan kejahatan elektronik.

Menurut Rene L. Pattiradjawane (2000), konsep hukum dari *cyberlaw*, *cyberspace* dan *cyberline* yang berkembang dari *computer crime* melahirkan

[18] Barda Nawawi, *Sari Kuliah: Perbandingan Hukum Pidana*, Cetakan I, (Jakarta: Raja Grafindo Persada, 2002). hlm 251-252

suatu ruang lingkup baru melalui jaringan internet yang dapat diakses setiap orang dengan jangkauan tanpa batas yang mengakibatkan keresahan bagi para penegak hukum untuk mengadakan regulasi khusus sebagai perlindungan terhadap pemilik data pribadi di *cyberspace*. Sedangkan menurut Jhon Sipropoulus kejahatan siber mempunyai sifat efisien dan akses yang cepat, sehingga menjadi tantangan yang sulit bagi pihak penegak hukum untuk melakukan mengungkapan terhadap pelaku kejahatan siber.[19]

b. Bentuk-bentuk Kejahatan Siber

Kejahatan siber memiliki spesialisasi khusus dalam melakukan tindak kejahatannya dan mengungkapan pelakunya, berbeda dengan kejahatan yang pada umumya dalam KUHP yang mana proses penggungkapan peristiwa dan pelaku dapat dilakukan dengan mengacu pada KUHAP. Kejahatan siber sendiri memerlukan suatu perangkat yang terhubung dengan internet untuk bisa melakukan tindak kejahatan. Kemampuan yang serbaguna dalam perkembangan teknologi yang tanpa batasan tertentu dan dampak yang timbul pun tidak secara langsung diketahui, sehingga menjadi atensi dalam melihat bentuk-bentuk terhadap kejahatan ini. Beberapa bentuk kejahatan siber yang berkaitan dengan data pribadi, sebagai berikut:[20]

1) *Malicious Software (Malware).*

[19] Galuh Kartiko, *Pengaturan Tehradap Yurisdiksi Cyber Crime Ditinjau dari Hukum Internasional,* Jurnal Rechtldee edisi No. 2, Vol. 8 Desember 2013, hlm 1

[20] Satriyo WIbowo, *Data Breach dan Tanggung Jawab Platform,* Seminar Online (webinar).

2) *Phising.*

3) *Man in the Middle Attacks.*

4) *Distributed Denial of Service (DDoS).*

5) *Cross-Site Scripting.*

6) *SQL Injection Attacks.*

7) *Miss-Autopaid.*[21]

Bentuk-bentuk dari kejahatan siber merupakan kemajuan teknologi dan informasi yang menimbulkan ancaman tidak hanya ditujukan terhadap orang tertentu tetapi bisa berdampak pada suatu negara. Risiko atas kejahatan siber berindikasi terhadap kerusakan dan kehilangan sistem informasi data dan gangguan jaringan komputer dan internet.

2. Kebijakan Hukum Pidana

Kebijakan hukum pidana sering diistilahkan *penal policy*, yang mana juga mempunyai pengertian yang serupa dengan istilah *criminal law policy* dan *strafrechtpolitiek* sehingga kedua istilah tersebut diterjemahkan sebagai politik hukum pidana atau kebijakan hukum pidana. Politik hukum pidana sebagai upaya yang rasional untuk menanggulangi kejahatan dengan menggunakan sarana hukum pidana yang menurut Marc Ancel merupakan suatu ilmu sekaligus seni dengan tujuan untuk memungkinkan peraturan hukum positif dirumuskan secara

[21] Luciana Dita, *Perlindungan Data Konsumen Dalam Perdagangan Secara Daring (Online Commerce),* Seminar Online (webinar).

baik dan juga kepada para penyelenggara atau pelaksana putusan pengadilan dapat diaplikasikan. Dengan demikian penerapan hukum pidana lebih dapat terukur bilamana keadilan bagi masyarakat terwujud sebagai rasa keadilan, sebab penyelenggaraan dan pelaksanaan peradilan akan berpegang pada pedoman yang lebih baik.[22]

Upaya negara (pemerintah) dalam menanggulangi kejahatan diantaranya melalui suatu kebijakan hukum pidana, pendapat Sudarto kebijakan hukum pidana meliputi dua hal, yaitu; a) Upaya mewujudkan peraturan-peraturan yang baik dengan keadaan dan situasi saat itu, b) Kebijakan dari negara melalui institusi yang berwenang dalam menetapkan suatu peraturan yang dikehendaki sebagai ekspresi apa yang terkandung dalam masyarakat untuk mencapai apa yang dicitakan.[23] Pendapat lain juga memaknai kebijakan kriminal sebagai bentuk yang diambil negara untuk melakukan kriminalisasi terhadap suatu tindakan yang dianggap merugikan, serta strategi untuk menanggulanginya. Sehingga kebijakan kriminal dimaknai sebagai pembuatan, pelaksanaan dan advokasi kebijakan yang oleh negara sebagai bentuk mengatasi masalah kejahatan.[24]

---

[22] H. Jhon Kenedi, *Kebijakan Hukum Pidana: Dalam Sistem Penegakkan Hukum Di Indonesia,* Cetakan Pertama, (Yogyakarta: Pustaka Pelajar, 2017), hlm 59.

[23] Ibid, hlm 61.

[24] Muhammad Mustofa, *Kriminolagi Kajian Sosiolagi Terhadap Kriminalitas, Perilaku Menyimpang dan Pelanggaran Hukum,* (Depok: Fisip UI Press, 2007), hlm 44.

Pada hakikatnya hukum pidana dan kegunaannya bertujuan agar setiap anggota masyarakat dapat dilindungi oleh hukum untuk tercapai jalan hidup yang sejahtera lahir dan batin. Berbagai upaya penegakkan hukum dalam rangka penanggulungan kejahatan, baik dengan cara tegas seperti pada Operasi Pemberantasan Kejahatan (OPK) di Indonesia awal tahun 1980-an sebagai langkah yang sangat keras sama sadisnya dengan kejahatan itu. Cara pencegahan kejahatan yang bersifat *"social treatment"* dan *"therapeutic"*, demikian pula dengan cara hukum yang *dogmatic legalistic* maupun tindakan hukum yang humanisme memang diperlukan kesungguhan dan kesadaran mengingat prosesnya yang relatif lama dan tidak semudah yang dibayangkan.[25]

Upaya pada pengunaan hukum pidana sebagai salah satu usaha untuk mengatasi masalah sosial termasuk dalam kebijakan penegakkan hukum maupun kebijakan di bidang sosial, yakni segala usaha yang rasional untuk mencapai kesejahteraan masyarakat. Sehingga sebagai suatu masalah termasuk kebijakan, maka penggunaan hukum pidana sebenarnya bukan merupakan suatu keharusan.[26] Menurut pendapat Muladi, penegakan hukum bukan sebagai harapan untuk menyelesaikan atau menanggulangi kejahatan secara tuntas. Hakikat kejahatan ialah "masalah sosial" dan "masalah kemanusiaan" yang

[25] M. Hatta, *Kebijakan Politik Kriminal; Penegakkan Hukum Dalam Rangka Penanggulangan Kejahatan,* Cetakan pertama, (Yogyakarta: Pustaka Pelajar, 2010), hlm 53.

[26] Barda Nawawi, *Kebijakan Legislatif Dalam Penanggulangan Kejahatan Dengan Pidana Penjara,* Cetakan keempat, (Yogyakarta: Genta Publishing, 2010), hlm 19.

bukan semata-mata hukum pidana untuk mengatasi masalah sosial. Fenomena kejahatan di masyarakat yang dinamis dan berkaitan dengan struktur kemasyarakatan lainnya yang sangat kompleks.

G. Metode Penelitian

1. Jenis Penelitian

   Penelitian ini menggunakan normatif, yang mengkaji hukum tertulis dari beragam perspektif, dan *library research* atau penelitian hukum kepustakaan untuk mendekati pokok masalah (isu hukum) berdasarkan berbagai kajian yang dapat ditelusuri, karena penelitian ini mendiskripsikan mengenai[27] kemampuan hukum pidana terhadap kejahatan siber terkait dengan perlindungan data pribadi di Indoensia, yang mana meliputi penegakan hukum dan kendala dalam menanggulangi kejahatan siber terkait perlindungan data pribadi di Indoensia..

2. Objek Penelitian

   Obyek penelitian ini berfokus terhadap permasalahan yang diteliti, sebagaimana yang terdapat pada rumusan masalah yakni:

   a. Kemampuan hukum pidana dalam menaggulangi kejahatan siber terkait perlindungan data pribadi.

[27] Muladi, *Kapita Selekta Sistem Peradilan Pidana,* (Semarang: Badan Penerbit Undip, 2004), hlm 7.

b. Kendala pada Undang-Undang Informasi dan Transaksi Elektronik dalam menanggulangi tindak pidana kejahatan siber terkait perlindungan data pribadi di Indonesia

3. Bahan Hukum

Penulisan tesis ini berdasarkan beberapa sumber baik dari bahan hukum primer dan didukung dengan bahan hukum sekunder serta bahan hukum tersier, yaitu:

a. Bahan Hukum Pimer

Bahan hukum pirmer adalah bahan hukum yang terdiri dari perundang-undangan, catatan-catatan resmi atau risalah pembuatan perundang-undangan[28]. Bahan hukum primer meliputi:

1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945
2) Kitab Undang-Undang Hukum Pidana
3) Undang-Undang Nomor 36 tahun 1999 tentang Telekomunikasi
4) Undang-Undang Nomor 39 Tahun 1999 Tentang Hak Asasi Manusia
5) Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik
6) Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan
7) Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan

[28] Mukkti Fajar dan Yulianto Achmad, *Dualisme Penelitian Normatif dan Empiris,* Cetakan pertama, (Yogyakarta: Pustaka Pelajar, 2009), hlm 140.

8) Undang-Undang Nomor 24 Tahun 2013 tentang Administrasi Kependudukan
9) Undang-Undang Nomor 30 Tahun 2014 Tentang Administrasi Pemerintahan.
10) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

b. Bahan Hukum Sekunder

Bahan hukum sekunder berfungsi sebagai menambah/memperkuat dan memberikan penjelasan terhadap data primer. Bahan hukum sekunder dalam penelitian ini meliputi:

1) Buku-buku yang memberikan penjelasan mengenai beberapa permasalahan hukum yang merupakan hasil yang bersinggungan mengenai penelitian termasuk seperti skripsi, tesis, dan disertasi
2) Jurnal ilmiah

c. Baham Hukum Tersier

Bahan hukum tersier merupakan bahan hukum yang mendukung dan memberikan petunjuk maupun penjelasan terhadap bahan hukum primer dan bahan hukum sekunder, seperti kamus hukum, kamus besar Bahasa Indonesia, ensiklopedia dan artikel dari media internet.

4. Pendekatan Penelitian

Penelitian hukum ini terdapat empat pendekatan yang digunakan. *Pertama*, pendekatan Undang-Undang (*statue approach)* dengan menelaah berbagai

Undang-Undang, regulasi, serta isu hukum yang berkaitan dengan objek penelitian, sehingga dapat dilihat konsistensi dan kesesuaian antara suatu Undang-Undang dengan Undang-Undang yang lain dan masih berlaku. *Kedua*, pendekatan konseptual *(conceptual approach)* yang berpijak pada pandangan-pandangan dan doktrin-doktrin yang berkembang dalam ilmu hukum. *Ketiga*, pendekatan historis *(historical approach)* pendekatan ini menelaah latar belakang perkembangan peraturan tentang kejahatan siber yang semakin berkembang terkait perlindungan data pribadi. *Keempat*, pendekatan kasus *(case approach)* dengan kasus terkait objek penelitian.[29]

5. Analisis Bahan Hukum

   Penelitian ini akan menguraikan masalah dengan menggunakan analisis deskriptif, yaitu dengan mengumpulkan semua data yang diperlukan terkait dengan penelitian, kemudian menghubungkan dengan permasalahan yang ada dan dianalisis berdasarkan teori hukum yang dihubungkan dengan masalah yang diteliti, kemudian data tersebut disistematiskan dan selanjutnya dianalisis untuk menjadi dasar dalam mengambil kesimpulan.

H. Sistematika Penulisan

Penulisan ini terdiri dari empat bab, dimana masing-masing bab memiliki keterkaitan antara yang satu dengan yang lain. gambaran yang lebih jelas mengenai penulisan hukum ini akan diuraikan dalam sistematika sebagai berikut:

[29] Peter Marzuki, *Penelitian Hukum,* tanpa cetakan, (Jakarta: Kencana, 2007), hlm 93-94.

Bab I pada bab ini memuat tentang latar belakang masalah, rumusan masalah, tujuan dan manfaat penelitian berisi uraian tentang tujuan dan manfaat yang ingin dicapai dalam penelitian ini, metode penelitian yang memuat tentang jenis penelitian, pendekatan penelitian, objek penelitian, data penelitian atau bahan hukum, pengolahan dan penyajian data penelitian dan analisis serta sistematika penulisan

Bab II, yaitu tinjauan pustaka. Bagian ini berisi uraian tentang landasan teori yang akan dijabarkan beberapa sub pembahasan. Terdapat empat sub bab, pertama Penegakan hukum, sub bab kedua kejahatan siber *(cybercrime)*, dan sub bab ketiga Perlindungan Data Pribadi.

Bab III akan membahas dan menganalisis meliputi:

1. Bagaimana kemampuan hukum pidana pada Undang-Undang Informasi dan Transaksi Elektronik dalam menanggulangi kejahatan siber terkait perlindungan data pribadi.
2. Seperti apa yang menjadi kendala pada Undang-Undang Informasi dan Transaksi Elektronik dalam menanggulangi kejahatan siber terkait perlindungan data pribadi di Indonesia.

Bab IV Penutup yang di dalamnya berisi tentang kesimpulan dan saran yang merupakan jawaban umum dari permasalahan yang ditarik dari hasil penelitian yang dirumuskan berdasarkan pembahasan pada Bab III dan saran-saran yang diharapkan dapat berguna bagi pihak terkait.

BAB II

TINJAUAN UMUM TENTANG PENEGAKAN HUKUM TERHADAP KEJAHATAN SIBER TERKAIT PERLINDUNGAN DATA PRIBADI

A. Penegakan Hukum

1. Pengertian dan Tahapan

Penegakan hukum merupakan istilah yang ruang lingkupnya cukup luas, tidak hanya perangkat negara sebagai penegak hukum yang bertanggungjawab secara langsung sebagai "*Law enforcement"* dalam arti penegakan hukum, tetapi termasuk "*Piece maintenance".*[30] Menurut pendapat Soekanto dalam bukunya Soerjono Soekanto, penegakan hukum memiliki konsep sebagai kegiatan menyelaraskan kandungan nilai-nilai yang dijabarkan dalam kaidah-kaidah sikap tindakan terhadap rangkaian penjabaran nilai tahap terakhir, untuk menciptakan, memelihara dan mempertahankan keadaan yang damai dalam masyarakat.[31] Mewujudkan suatu perilaku dan sikap tindak sebagai tujuan untuk menciptakan, memelihara, dan mempertahankan perdamaian di masyarakat merupakan realitas dari penegakan hukum secara konseptual.[32]

---

[30] Moh. Hatta, *Beberapa Masalah Penegekan Hukum Pidana Umum dan Pidana Khusus,* Cetakan pertama (Yogyakarta; Liberty, 2009). hlm 73.

[31] Soerjono Soekanto, *Faktor-faktor Yang Memperngaruhi Penegakan Hukum,* edisi pertama, (Jakarta; Raja Grafindo Persada, 2007). hlm 5.

[32] Ibid, hlm 7.

Penegakan hukum tidak hanya sebagai pelaksanaan perundang-undangan, meskipun di Indonesia realitasnya dianggap seperti itu. Disisi lain, penegakan hukum juga diartikan sebagai pelaksanaan keputusan-keputusan hakim *(inkracht)*. Pengertian yang secara sempit tersebut mempunyai kelemahan dalam pelaksanaan perundang-undangan atau keputusan-keputusan hakim tersebut dapat menjadi kendala dan mengganggu di masyarakat. Penjelasan penegakan hukum diatas memperlihatkan faktor-faktor yang mungkin mempengaruhi citra ideal dari penegakan hukum itu sendiri. Beberapa faktor yang mempengaruhi sebagai berikut:[33]

a. Faktor hukum, artinya hanya dibatasi pada undang-undang saja
b. Faktor penegak hukum, pembentuk maupun penerapan hukum
c. Faktor sarana dan prasarana pendukung
d. Faktor masyarakat, lingkungan dimana hukum itu diterapkan
e. Faktor kebudayaan yang melatarbelakangi krasa manusia dalam kehidupan sosial.

Penegakan hukum pada prinsipnya mengarah pada nilai-nilai yang terdapat pada hukum sebagai gambaran yang harus memberikan kepastian hukum *(Rechtssicherheit)*, kemanfaatan *(zweckmassigkeit)*, dan keadilan *(gerechtigkeit)*, yang dapat dimaknai sebagai berikut:[34]

[33] Ibid, hlm 8.

[34] Sudikno Mertokusumo, *Mengenal Hukum: Suatu Pnegatar,* cetakan lima, (Yogyakarta: Cahaya Atma Pustaka, 2003), hlm 207-208.

a. Kepastian hukum dianggap sebagai pelindung yustisiabel berkenaan pada tindakan sewenang-wenang, artinya setiap orang dapat mendapatkan suatu yang diharapkan dalam keadaan tertentu sebagai bentuk adanya kepastian hukum kerena adanya hal tersebut masyarakat akan lebih tertib. Tujuan dari hukum untuk ketertiban masyarakat.
b. Kemanfaatan dalam hal ini adanya faedah terhadap pelaksanaan atau penegakan hukum. Artinya dengan penegakan hukum ada nilai guna bagi masyarakat, jangan sebaliknya malah timbul keresahan di dalam masyarakat.
c. Keadilan, dalam pelaksanaan penegakan hukum adanya keadilan diperhatikan bagi masyarakat yang mengikat setiap orang untuk menyetarakan, tidak adanya perbedaan dalam memberikan porsi yang sesuai dengan tindakan yang menyimpang.

Ketiga komponen tersebut tercermin melalui proses penegakan hukum yang harus dijadikan tujuan utama dalam penegakan hukum. Jika sebaliknya bila yang diperhatikan hanyalah kepastian hukum saja dimana komponen lain diabaikan, maka orang tidak mengetahui apa yang diperbuat dan akhirnya munculnya keresahan. Terlalu menitikberatkan pada kepastian hukum, terlalu mentaati peraturan hukum, maka terlihat kaku dan bisa muncul rasa ketidakadilan. Hal apapun yang terjadi bila peraturannya demikian dan harus ditaati atau dilaksanakan secara ketat seperti adagium "*lex dura, sed tamen*

scripta (undang-undang itu kejam, tetapi memeng seperti itu bunyinya).[35] Sehingga perlu diperhatikan secara proposional keseimbangan dalam melihat pelaksanaan penegakan hukum. Meskipun praktiknya tidak selalu mudah mengusahakan kompromi secara tepat terhadap keseimbangan dari komponen tersebut pada penegakan hukum.

Penegakan hukum menurut pendapat Barda Nawawi merupakan upaya menanggulangi kejahatan secara rasional, sesuai dengan rasa keadilan dan berdaya guna bagi masyarakat. Usaha menanggulangi kejahatan melalui berbagai sarana sebagai respon terhadap tindakan pelaku kejahatan, dan dapat berupa sarana hukum pidana atau non-hukum pidana yang dapat diintegrasikan. Penanggulangan kejahatan yang dipilih adalah hukum pidana sebagai sarana menanggulangi kejahatan, maka perlu dilakukan sesuai dengan politik hukum pidana sesuai dengan keadaan (budaya dan nilai di masyarakat) dan situasi saat ini dan dapat menjangkau untuk masa depan.[36]

Pengertian penegakan hukum berdasarkan beberapa pendapat diatas dapat dimaknai penegakan hukum sebagai upaya untuk menjalankan dan menerapkan fungsi-fungsi dari norma-norma hukum secara nyata yang mengatur dan menghubungkan hukum dengan masyarakat sesuai dengan kebutuhan dan dapat diterapkan serta menjadi pedoman terhadap

[35] Ibid. hlm 209

[36] Barda Nawawi Arief, *Kebijakan Hukum Pidana*¸ cetakan -----, (Bandung; Citra Aditya Bakti, 2002), hlm 109.

perkembangan masyarakat. Penegakan hukum diharapakan dapat memberikan jaminan terwujudnya kepastian hukum, ketertiban masyarakat, dan adanya perlindungan hukum, sehingga dapat menjaga keseimbangan dan keselarasan antara moral yang berlandaskan pada nilai-nilai dalam bermasyarakat.

Penegakan hukum juga dapat ditinjau dari 2 hal, yakni **sudut subyek dan sudut objeknya**, yakni: [37]

a. Dilihat dari sudut subyeknya dilakukan oleh subyek secara luas dan dapat pula diartikan sebagai upaya penegakan hukum oleh subyek yang terbatas atau sempiit. Luas disini dimaknai sebagai proses penegakan hukum yang melibatkan semua subyek hukum yang memiliki keterkaitan dan hubungan hukum baik yang menjalankan aturan bersifat normatif atau melaksanakan sesuatu atau tidak yang berdasarkan pada aturan hukum yang berlaku sebagai bentuk mematuhi atau menegakkan aturan yang berlaku. Sedangkan dalam arti sempit dari sudut subyeknya sebagai upaya aparatur atau instrumen penegakan hukumnya saja untuk menjamin dan memastikan sutau aturan hukum berjalan sesuai dengan yang dicitakan. Instrument atau aparatur penegak hukumnya diberikan kewenangan menggunakan daya paksa dalam memastikan berlakunya dan tegaknya

[37] Jimly Asshidiqie, dalam http://www.jimly.com/makalah/namafile/56/Penegakan_Hukum.pdf , diakses pada tanggal 13 Oktober 2020, hlm 1-2.

hukum sebagai upaya bila diperlukan. Ditinjau dari sudut objeknya, mencakup makna yang luas dan sempit. Penegakan hukum juga mencakup nilai-nilai keadilan yang terkandung di dalamnya bunyi aturan baik formal maupun nilai-nilai keadilan yang hidup dalam masyarakat. Tetapi dalam arti sempit dimaknai hanya berkaitan pada penegakan peraturan yang bersifat tertulis saja. Bahasa Indonesia menerjemahkan 'penegakan hukum' dalam arti luas dan 'peraturan penegakan hukum' dalam arti sempit dari kata *"law enforcement".* Perbedaan itu sendiri muncul dari dalam bahasa Inggris yang dikembangkan dari *'the rule of laws'* dan *'the rule of just law'* atau dalam istilah *'rule of law and not of man'* dengan istilah *'the rule by law'* yang berarti the '*rule of man by law'*. Isitilah '*the rule of law'* bermakna pemerintahan oleh hukum, tetapi bukan dalam arti formal yang melainkan mencakup nilai-nilai keadilan, maka digunakan istilah *'the rule of just law'.* Penegasan dalam isitilah '*the rule of law and not of man'* hakikatnya bermakna pemerintahan suatu negara hukum modern dilakukan oleh hukum, bukan oleh orang. Begitu sebaliknya *'the rule by law'* sebagai maksud pemerintahan yang dilakukan oleh orang dengan sarana hukum hanya untuk alat kekuasaan belaka.

b. Secara objektif penegakan hukum mencakup hukum formal dan hukum material. Hukum formal hanya berkaiatan dengan peraturan perundang-undangan yang tertulis, sedangkan hukum material melingkupi nilai-nilai keadilan yang hidup di masyarakat. Meskipun secara Bahasa, penegakan

hukum membedakan antara penegakan hukum dengan penegakan keadilan, apabila dikaitkan penegakan hukum secara sempit serupa dengan istilah *law enforcement*, berbeda dengan istilah penegakan keadilan yang diartikan luas meliputi hukum material dalam penegakan hukum.

Penegakan hukum juga dimaknai dengan 2 cara yang secara umum banyak dikenal dengan cara preventif *(preventive)* dan represif *(repressive)* atau sarana penal dan non-penal. Penegakan hukum secara preventif dilakukan dengan mencegah tanpa adanya pidana *(prevention without punishment/mass media)* yang mana lebih menitik beratkan pada sifat mencegah sebelum terjadi suatu tindak pidana. Sedangkan represif *(represive0* juga dapat dipandang preventif secara luas, artinya sebelum preventif disini lebih bersifat mencegah terhadap keadaan penyebab terjadinya pelanggaran, dengan melihat kondisi sosial secara langsung dan tidak langsung dapat menimbulkan atau menyuburkan suatu tindakan kejahatan, ketika hal demikian terjadi dan tidak bisa dibendung lagi maka upaya yang dilakukan adalah pemidanaan.[38]

Aspek lain yang juga perlu diperhatikan adalah aspek perlindungan terhadap masyarakat yang harus diperhatikan dalam penegakan hukum pidana, terdiri dari 4 (empat) hal, yaitu:[39]

---

[38] Barda Nawawi, *Bunga Rampai Kebijakan Hukum Pidana,* cetakan kelima, (Jakarta: Kencana, 2016), hlm 46.

[39] _____, *Beberapa Aspek Kebijakan Penegakan dan Pengembangan Hukum Pidana,* cetakan pertama, (Bandung: Citra Aditya Bakti, 1998), hlm 13.

a. Perlunya perlindungan bagi masyarakat terhadap perbuayan anti sosial yang berindikasi merugikan dan membahayakan masyarakat. Sehingga tujuan dari penegakan hukum untuk menanggulangi kejahatan.
b. Perlindungan yang bersifat berbahayanya seseorang pada masyarakat. Sehingga lumrah tujuan dari penegakan hukum pidana sebagai sarana memperbaiki si pelaku kejahatan atau berusaha mengubah dan mempengaruhi tingkah lakunya ke arah yang tidak menyimpang dan menjadi masyarakat yang baik dan berguna.
c. Perlindungan dari penyalahgunaan sanksi atau reaksi dari penegak hukum kepada masyarakat itu sendiri, secara logis untuk menghindari tindakan penyalahgunaan wewenang yang sewenang-wenang di luar hukum.
d. Perlunya perlindungan terhadap keseimbangan atau keselarasan dari syarat kepentingan dan nilai yang terganggu dari akibat adanya kejahatan. Maka dari itu penegakan hukum pidana menjadi solusi menyelesaikan konflik yang muncul dari tindak pidana serta memulihkan keseimbangan dan terwujudnya rasa damai dalam masyarakat.

Wujud dari penegakan hukum sebagai sarana untuk dapat memberikan solusi dari berbagai konflik yang timbul di masyarakat, yang mana masalah tersebut dilakukan dan dianggap sebagai tindak pidana. Sehingga pemulihan dengan penegakan hukum sesuai dengan idealitasnya untuk menciptakan ketertiban di masyarakat.

2. Efektivitas dan Faktor Penegakan Hukum

Berbicara tentang masyarakat tentu tidak dapat terhindar dari pembicaraan mengenai kehadiran teknologi ditengah-tengah masyarakat modern. Beragam karakteristik teknologi modern bisa dilihat dari percepatannya, daya pelipatannya, dan juga kemampuannya merusak berlipat ganda daripada berbagai penemuan manusia sebelumnya. Perubahan yang cepat tentu mempengaruhi pola-pola hubungan dalam masyarakat, mulai dari perubahan nila-nilai, arahan, kehidupan, sampai pada struktur sosial dan lembaga-lembaga dalam masyarakat. Penegakan hukum bukan hanya kegiatan yang semata-mata berdiri sendiri, tetapi senantiasa adanya kegiatan dengan masyarakat sebagai bentuk pelayanan atau istilah Parsons bila dikutip "*relational"*.[40] Faktor perubahan pada masyarakat akibat kemajuan teknologi sangatlah berpengaruh terhadap penegakan hukum yang ada dalam masyarakat.

Peranan kemajuan teknologi dapat menimbulkan pengalaman psikologis tersendiri terhadap masyarakat, penegak hukum, dan norma-norma yang ada dalam masyarakat, tentunya juga membutuhkan penyesuaian tersendiri yang tidak mudah dilakukan. Keberadaan teknologi pun seharusnya bisa dimanfaatkan untuk mengatur masyarakat, mengatur disini dimaknai sebagai '*social engineering'.*

[40] Satjipto Raharjo, *Masalah Penegakan Hukum; Suatu Tinjauan Sosiologis"*, tanpa cetakan, (Bandung: Sinar Baru, 1983), hlm 123.

Penegakan hukum modern menurut pendapat Trubek dibagi menjadi tiga pokok cirinya:[41]

a) Merupakan sistem peraturan-peraturan
b) Sebagai suatu bentuk kegiatan manusia yang dilakukan dengan sadar untuk mencapai tujuan
c) Ia serentak merupakan bagian dari, tetapi juga terlepas *(autonomous)* dari negara.

Ciri dari hukum modern ialah identitasnya sebagai bentuk kegiatan manusia yang dilakukan secara sadar untuk mencapai suatu tujuan, lalu hukum menjadi instrumental sifatnya.[42]

3. Beberapa Prinsip dan Asas penegak hukum

Konsep penegakan hukum perlu dipahami secara baik *(good law enforcement)*, dan memahami prinsip-prinsip di dalamnya. Tolak-ukur kinerja sutau penegakan hukum dapat terlihat baik atau kurang berjalan apabila pelaksanaannya telah mencakup dengan semua unsur prinsip-prinsip penegakan hukum yang baik, mengacu pada prinsip-prinsip demokrasi beserta elemen-elemennya, semisal legitimasi, akuntabilitas, perlindungan hak asasi manusia, kebebasan, transparansi, pembagian kekuasaan dan kontrol dari masyarakat.[43] Pentingnya memahami penegakan hukum guna menilai kinerja

[41] Ibid, hlm 116.
[42] Ibid, hlm 117.
[43] Kusnu Goesniadhie, *Perpsektif Moral Penegakan Hukum yang Baik,* Jurnal Hukum, Vol. 17, No. 2 2017, hlm 206.

dari para penegak hukum itu sendiri dan didayagunakan secara efektif melaksanakan kontrol sosial dengan optimal, sehingga menjadi harapan kualitas keputusan-keputusan yang dihasilkan dapat merefleksikan *predictability*, *accountability*, *transparency*, dan *widely participated.*[44]

Problem yang timbul dalam penegakan hukum ialah didominasi dengan menggunakan pendekatan hukum pidana yang mengarah pada *overkriminalisasi* dan *overpenalisasi*, sehingga dapat berakibat hukum pidana tidak berjalan sesuai dengan ide awal dan tujuan dari penggunaan pidana itu sendiri. Bahkan hilangnya wibawa dan fungsi hukum pidana dalam masyarakat.[45]

Beberapa prinsip untuk menghindari dari *under and overcriminalization* berkaitan dengan penegakan hukum pidana yang dibuat oleh *Organizatiion fot Economic Co-Operation and Development (OECD)*, sebagai berikut:[46]

a) Ultima ratio principle, hukum pidana sebagai sarana terakhir atau senjata pamungkas *(ultimum remedium)*, realitanya penggunaan hukum lebih tendensi pada *primum remediun* atau mengedepankan hukum pidana dalam mengatasi problem sosial. Pidana denda bahkan menjadi salah satu sanksi sebagai sumber dana pembangunan negara.

[44] Ibid, hlm 207.

[45] Roeslan Saleh, *Beberapa Asas Hukum Pidana Dalam Perspektif,* Tanpa Cetakan, (Jakarta: Aksara Baru, 1983), hlm 46.

[46] Teguh Prasetyo, *Kriminalisasi Dalam hukum Pidana,* cetakan pertama, (Bandung: Nusa Media, 2010), hlm 40-41.

b) *Precision principle,* ketelitian dan ketepatan dalam ketentuan hukum pidana untuk mengdiskripsikan suatu perbuatan tindak pidana. Sehingga dalam formulasi tindak pidana yang samar dan rancu dapat terhindar.

c) *Cleaness principle*, rumusan pengaturan mengenai tindakan yang dikriminalisasikan harus dijabarkan dan dijelaskan secara mendetail dalam ketentuan tindak pidana.

d) *Principle of differentiation,* perbedaan antara satu sama lain pada formulasi perbuatan pidana harus jelas, agar terhindar pasal-pasal yang bersifat global atau pemaknaannya yang luas, *multipurpose* atau *all embracing.*

e) *Principle of intent*, perumusan untuk mengkriminalisasikan suatu tindak pidana harus jelas dolusnya, sedangkan culpa dinyatakan dengan syarat khusus untuk memberikan pembenaran mengkriminalisasikan suatu tindak pidana.

f) *Principle of victim application*, pada prinsip ini perlu diperhatikan permintaan atau kehendak korban kejahatan dalam penyelesaian perkara pidana, karena hal ini demi kepentingan korban dalam rangka pembinaan dan pemidanaan terhadap pelaku.

Asas-asas hukum merupakan pikiran yang fundamental yang berada di dalam dan di belakang sistem hukum, masing-masing dirumuskan dalam aturan perundang-undangan yang berkaitan pada ketentuan dan keputusan-

putusan yang dipandang sebagai penjabarannya.[47] Pemikiran dasar yang umum dan abstrak dari asas hukum merupakan petunjuk berlakunya hukum, dan penting serta *principle*. Penguasaan aspek-aspek filsafat hukum, teori hukum dan norma-norma hukum kurang memadai untuk memberikan jaminan atas kualitas penegakan hukum, tanpa adanya pemahaman terhadap asas hukum yang baik, maka perlu dalam penegakan hukum asas-asas hukum diuraikan sebagai berikut:

a) Asas Legalitas

Kedudukan hukum sebagai *supremacy* menjadi ciri dari suatu negara hukum yang mengatur pelaksanaan kehidupan negara, pelaksanaan oleh para penguasa negara dalam menjalankan tugas dibatasi, dengan tujuan untuk memberikan jaminan terseleanggaranya kepentingan rakyat. Maka setiap tindakan dari penguasa harus patuh dan taat sesuai dengan hukum begitu juga setiap warga negara di dalamnya. Negara memiliki kewenangan dan tindakan yang berdasarkan pada hukum dan sifat hukum itu sendiri, dalam mewujudkan jaminan terhadap hak asasi dan hal-hal yang berpihak pada kepentingan rakyat., yang timbul secara demokratis, dan

[47] Dewa Gede Atmadja, *Asas-asas Hukum dalam Sistem Hukum,* jurnaa Kertha Wicaksana, Vol. 12, No. 2 2018, hlm 146.

dilakukan dengan cara-cara yang sah, serta adanya kontrol dalam penegakannya melalui sistem yang konstitusional.[48]

Hukum pidana sebagai instrumen dalam penegakan yang diselenggarakan oleh penguasa (aparat penegak hukum) tidak dapat lepas dari ciri dan asas-asas yang berlaku di negara hukum. Legalitas hukum pidana di suatu negara dipengaruhi oleh keberadaan asas legalitas dalam hukum pidana itu sendiri, dan asas yang berlaku secara *universal* yang menentukan bahwa tidak ada suatu perbuatan dilarang dan diancam dengan pidana, jika tidak ditentukan terlebih dahulu dalam perundang-undangan. Menurut Von Feuerbach ahli hukum pidana jerman yang juga ikut merumuskan pokok pikiran mengenai asas legalitas dengan adagium yang dikenal "*nullum delictum nulla poena sine praevia lege"* (tidak ada suatu perbuatan dapat dipidana, jika perbuatan tersebut diatur terlebih dahulu).[49]

Kebaradaan asas legalitas dalam hukum pidana di Indonesia terdapat dalam Pasal 1 ayat (1) KUHP yang mana letaknya pada Bab I yang bersifat abstrak dalam aturan umum. Sehingga menggambarkan bahwa asas legalitas yang keberadaannya menjadi sentral dan fundamental. Setidaknya ada tiga pengertian pokok dalam asas legalitas, yakni:[50] *pertama*, tidak ada

[48] Bambang Poernomo, *Hukum Pidana Kumpulan Ilmiah,* Cetakan pertama, (Jakarta: Bina Aksara, 1982), hlm 28-29.

[49] Moeljatno, *Azas-azas Hukum Pidana,* Cetakan keempat, (Jakarta: Bina Aksara, 1987), hlm 23.

[50] Moeljatno, loc. cit.

perbuatan yang dilarang dan diancam pidana, jika hal itu telah diatur terlebih dahulu sebelum dinyatakan dalam suatu perundang-undangan, *kedua* tidak diperbolehkan menggunakan analogi, dan *ketiga* aturan pidana tidak berlaku surut.

Para ahli hukum pidana pada umumnya menolak bila menggunakan analogi, sebab dapat menimbulkan kesesatan dan tidak memberikan kepastian hukum tentang suatu perbuatan yang dilarang dan yang diperbolehkan. Penggunaan analogi pada Pasal 1 ayat (1) KUHP dapat bermakna memperluas rumusan suatu delik.[51]

b) Asas Kekhususan Sistematis

Istilah *administrative law* dalam konteks hukum pidana merupakan produk legislasi berbentuk perundang-undangan, yang dalam hal ini adminsitrasi negara yang memuat sanksi pidana di dalamnya.[52] Disamping itu hukum administrasi disebut sebagai "hukum mengatur atau hukum pengaturan". Asas kekhususan sistematis merupakan upaya mengharmonisasi dan mensinkronisasi antar perundang-undangan yang terkandung sanksi pidana didalamnya, baik bersifat *pure criminal act* ataupun hukum pidana administrasi *(administrative law)*. Dalam hal ini asas kekhususan sebagai ketentuan pidana yang bersifat khusus apabila

[51] Leden Marpaung, *Asas-Teori-Praktik Hukum Pidana,* cetakan ketujuh, (Jakarta: Sinar Grafika, 2012), hlm 5.

[52] Indariyanto Seno Adji, *Keorupsi dan Penegakan Hukum,* cetakan pertama, (Jakarta: Dadit Media, 2009), hlm 155.

pembentukan suatu perundang-undangan memang bertujuan untuk memberlakukan ketentuan hukum pidana sebagai suatu aturan yang bersifat khusus atau akan bersifat khusus dari kekhususan yang telah ada.[53]

Bentuk perundang-undangan pada hukum pidana di luar kodifikasi (*lex specialis)* yang memberikan kekhususan terhadap tindak pidana yang berlainan dengan yang umum *(lex generalis)* sebagai alternative yang kian kompleks mengenai hukum pidana yang berkembang. Dalam hal ini untuk menentukan kekhususan pada hukum pidana di luar kodifikasi hukum pidana yang dinamis dan limitative sifatnya maka perlu dilihat undang-undang khusus mana dapat diberlakukan dan seperti apa ketentuan yang diterapkan dalam undang-undang khusus tersebut.[54]

Berlakunya asas *systematische specialiteit* dalam penentuan dalam undang-undang khusus yang diberlakukan dimaknai sebagai ketentuan pidana yang sifatnya khusus bila tujuan dari pembentukan undang-undang tersebut dimaksud memberlakukan ketentuan pidana yang bersifat khusus atau sifatnya khusus dari yang telah ada. Semisal dalam hal ini yang sifatnya khusus mengenai subyeknya, obyek yang dianggap perbuatan

[53] Marchelino Cristian N, *Penerapan Asas Kekhususan Sistematis sebagai Limitasi antara Hukum Pidana dan Hukum Pidana Administrasi,* Jurnal Hukum Unsrat edisi No.10, Vol. 23 desember 2018, hlm 57.

[54] Indariyanto Seno Adji, op.,cit, hlm 170-171.

tercela, alat bukti sebagai pembuktian yang dilakukan, ruang lingkup dan delictnya.[55]

Penentuan ketentuan pasal yang ditentukan terhadap undang-undang khusus juga berlaku asas *logische specialiteit* atau kekhususan yang logis, diartikan sebagai perbuatan pidana yang bersifat khusus apabila ketentuan pidana selain yang telah termuat unsur-unsur lain, juga semua unsur ketentuannya bersifat umum.[56]

c) Asas Subsidiaritas

Asas subsidair atau subsidiaritas yang dikenal *alternative second* sebagai upaya penerapan hukum pidana bukan yang utama dalam menanggulangi kejahatan.[57] Artinya hukum pidana sebagai jalan terakhir atau pamungkas *(ultimum remediaum)* yang mana dalam penyelesaian terhadap suatu perbuatan yang menyimpang tidak dapat digunakan lagi selain hukum pidana meski telah menggunakan pendekatan hukum lainnya. Sebelum perbuatan tersebut dinyatakan sebagai perbuatan pidana, maka perlu melihat apa yang menjadi kepentingan hukum yang dilanggar atau merugikan atas perbuatan tersebut yang dapat dilindungi, diselesaikan, dan dicegah. Sehingga pendekatan pidana dapat digunakan di keadaan

[55] Ibid.
[56] Ibid.
[57] Rusli Muhammad, *Sistem Peradilan Pidana Indonesia,* Cetakan pertama, (Yogyakarta; UII Press, 2011), hlm 12.

tertentu yang mana cara-cara yang digunakan dengan pendekatan sosial lainnya tidak efektif.[58]

Gagasan mengenai *ultimum remedium* pada hukum pidana menurut Brissot berlandaskan pada pemikiran prevensi secara garis besar menyebutkan lebih utama mencegah suatu perbuatan kejahatan dari pada harus memidanakannya. Sebab mengatasi kejahatan tidaklah harusnya menggunakan hukum pidana apabila itu merupakan symptom dari masalah sosial, lebih baik menggunakan suatu politik sosial.[59]

Penggunaan hukum pidana menurut cendekia hukum pidana haruslah menahan diri dan detail, dari aspek pembentukan undan-undangnya maupun pada implementasi hukum pidana dalam pelaksanaannya (penegakan hukum). Keyakinan yang berkembang mengenai hukum pidana itu sendiri sebagai pemotong daging sendiri juga mengarah pada dapat mengganggu. Pada akhirnya penggunaan hukum pidana sebagai solusi yang benar-benar tidak dapat dihindari lagi.[60] Dalam hal ini pendekatan hukum dalam penyelesaian yang diinginkan dengan sanksi di bidang hukum meliputi administrasi dan sanksi perdata tidak efektif lagi

[58] Mardjono Reksodiputro, *Menyelaraskan Pembaruan Hukum,* cetakan pertama, (Jakarta: Komisi Hukum Nasional, 2009), hlm 99.

[59] Roeslan Saleh, *Beberapa Asas Hukum Pidana Dalam Perspektif,* Tanpa Cetakan (Jakarta: Aksara Baru, 1983), hlm 47-49.

[60] _____, *Segi Lain Hukum Pidana,* cetakan pertama, (Jakarta: Ghalia Indonesia, 1984), hlm 16.

atau kesalahannya relative berat atau menimbulkan kegaduhan di masyarakat.

B. *Cybercrime*

1. Pengertian dan Konsep

Perkembangan di bidang teknologi informasi dan komunikasi memungkinkan orang untuk menggunakan internet melalui komputer pribadi *(personal computer/PC)* atau media elektronik lainnya, pemanfaatan teknologi digunakan oleh pribadi, korporasi, pemerintah, dan kelompok-kelompok masyarakat dalam berbagai aktivitas manusia. Disisi lain, kemajuan internet timbul hal lain seperti kejahatan di dunia internet di era sekarang yang menjadi atensi sebagai dampak perkembangan teknologi yang begitu pesat.

Isitilah yang digunakan tindak pidana kejahatan komputer dalam Bahasa inggrispun sangat bermacam-macam. Banyak istilah yang digunakan seperti *"computer misuse", "computer abuse", "computer crime", "computer fraud", "computer-related crime",* dan *"computer-assisted crime".* Namum pada umumnya lebih banyak diterima dengan memakai istilah "*computer crime"*, karena dianggap lebih luas dan telah lazim digunakan dalam hubungan internasional. Di negara Amerika contohnya menggunakan *"computer-related crime"* oleh *The U.S Computer Crime*. Sebaliknya penggunaan istilah *'computer misuse'* lebih tepat dari pada *'computer crime'* karena sifatnya lebih membatasi pada perbuatan yang dilarang oleh undang-undang hukum pidana oleh Komisi Franken, meskipun perbuatan

penyalahgunaan komputer juga dapat dilarang oleh undang-undang lainnya. Melihat istilah yang digunakan di Belanda dengan menyebut *'computer misbruik'* disamping *'computer criminaliteit'*. Di Indonesia sendiri istilah yang digunakan ialah penyalahgunaan komputer atau kejahatan komputer. Tapi istilah yang tampaknya lebih cocok ialah kejahatan komputer, karena penyalahgunaan komputer memiliki pengertian bahwa komputer merupakan alat untuk melakukan tindak pidana, padahal dalam kenyataannya komputer dan data komputer yang menjadi objek dari tindak pidana. Meski begitu kejahatan komputer memiliki pengertian yang lebih luas yaitu tindak pidana dimana komputer selain sebagai sarana untuk melakukan suatu tindak pidana, juga sebagai objek dari tindak pidana itu sendiri.[61]

Kejahatan siber *(cyber crimes)* dimaknai sebagai kejahatan komputer yang dilakukan di *"cyberspace"* (alam siber), yakni dimana adanya ruang tersendiri yang muncul berbagai transaksi niaga dan informasi lainnya yang berharga di *cyberspace* tersebut atau sering disebut swalayan-cyber. Konsep dari ruang siber *(cyberspace)* sendiri dimaknai sebagai ruang yang terhubung dan saling terkomunikasi menggunakan jaringan internet dalam melakukan aktifitas.[62] Istilah *Cyberspace* berasal dari kata yang diambil dari data *cybermetics*, yang mulanya *cyberspace* tidak menggambarkan interaksi melalui jaringan

[61] Puslitbang Hukum dan Peradilan, *Naskah Akademis Kejahatan Internet (cyber crimes)*, Mahkamah Agung, 2004, hlm 7.

[62] Kementrian Pertahanan Indonesia, *Pedoman Pertahanan Siber*, cetakan …. (Jakarta: Kemenhan RI, 2014), hlm 5.

komputer.[63] *Cyber* dan teknologi bila ditelusuri berasal dari asal kata *technique*, dalam bahasa Yunani Tecknikos yang artinya kesenian atau keterampilan dalam dan logos adalah ilmu atau asas-asas utama pada *cyber (software).*[64]

Pengertian kejahatan komputerpun dari beberapa sarjana hukum dibagi menjadi 2 (dua) pengertian, baik pengertian secara luas dan yang lainnya secara sempit, dapat dilihat sebagai berikut:

a. Pengertian secara sempit yang dipandang bahwa kejahatan komputer definisinya sebagai "tindak pidana yang dilaksanakan dengan menggunakan teknologi canggih, tanpa penguasan ilmu yang mana tindak pidana tidak mungkin dapat dilaksanakan.[65] Menurut Donn Parker dan Nycum yang menganut pengertian sempit memberikan uraian secara umum terkait kejahatan siber yang mana *computer crime* yang digunakan sebagai kegiatan kejahatan adalah komputer, sedangkan *cybercrime* alat yang digunakan sebagai kejahatan melalui *cyberspace*. Departement Hukum Amerika Serikat melihat kejahatan siber sebagai jenis kejahatan *any/illegal act requiring knowledge of computer technology for its perpetration, investigation, or prosequtio*n atau kejahatan yang mana

[63] Inue Rahmawati, *Analisis Manajemen Resiko Ancaman Kejahatan Siber,* Jurnal Pertahanan & Bela Negara, Vol. 7, No. 2 Agustus 2017, hlm 55.

[64] Sugeng Brantas, *Defence Cyber dalam Konteks Pandangan Bangsa Indonesia tentang Perang dan Damai*, Jurnal Pertahanan Vol. 2, No. 2 2014. hlm 55.

[65] Puslitbang Hukum dan Peradilan, op., cit, hlm 9.

manusia sebagai pelaku dengan menggunakan komputer yang terhubung pada jaringan internet.

b. Beberapa sarjana yang menganut pengertian luas ialah Comer yang memberikan pengertian bahwa kejahatan komputer sebagai "setiap perbuatan yang dilakukan dengan itikad buruk untuk tujuan keuangan yang melibatkan komputer. Sedangkan The British Law Commission mengartikan *"computer fraud"* sebagai "cara apapun yang dilakukan dengan ithikad buruk untuk memperoleh uang, barang atau keuntungan lainnya atau dimaksudkan menimbulkan kerugian kepada pihak lain dengan memanipulasi komputer".

Definisi kejahatan siber hingga saat ini pun belum secara tegas adanya kesepakatan dari berbagai pakar keilmuan, sebab kejahatan siber merupakan kegiatan yang memliki ruang lingkup dan aktivitas yang luas ditambah kemajuan teknologi yang pesat menjadikan sulit untuk menginterpretasikan definisi dari kejahatan tersebut.[66] Komisi Franken dari Belanda dan Komisi Inggris yang bertugas menyusun rencana undang-undang tidak memberikan pengertian yang jelas mengenai apa kejahatan komputer itu, dalam rencana undang-undang tersebut memang disebutkan beberapa perbuatan penyalahgunaan komputer yang tidak dapat dijangkau oleh undang-undang

[66] Sinta Dewi, *Cybercrime Dalam Abad 21: Suatu Perspektif Menurut Hukum Internasional,* Jurnal MMH Edisi 40, No. 4 Oktober 2011. hlm 525.

hukum pidana yang berlaku. Sehingga tidak terlihat adanya penggunaan definisi mngenai kejahatan komputer, bahkan usulan untuk membuat definisi mengenai "komputer", "data", dan "program" tidak mendapat persetujuan sebab mengingat pesatnya perkembangan teknologi informatika dikhawatirkan dari pendefinisan tersebut tidak akan sesuai lagi dengan perkembangan baru yang muncul, maka diserahkan kepada pengadilan untuk memberikan pengertiannya.[67] Istilah dari kejahatan komputer atau kejahatan siber dirasa perlu untuk memberikan suatu pengertian sebagai gambaran yang seragam, sehingga dalam hal terkaitdapat mempermudah sebagi studi ilmiah, pratik hukum di lapangan (penyidikan dan penuntutan) dan mempermudah penyusunan statistic pidana, yang dapat diketahui sejauh mana termasuk dalam kejahatan komputer.

2. Bentuk-bentuk Kejahatan Siber

Kejahatan siber semakin beragam seiring dengan perkembangan teknologi internet. Kejahatan siber muncul disebabkan adanya komunikasi dan terkoneksi antara komputer/perangkat elektornik satu dengan perangkat lainnya melalui suatu jaringan, serta dapat memberikan sesuatu antara satu sama lain, bahkan bisa mengendalikan pihak lain. Bentuk serangan siber yang menjadi popular/tren bagi para pelaku serangan siber dengan serangan *malware* atau yang lebih dikenal *Project Sauron*, umumnya serangan *malware*

[67] Puslitbang Hukum dan Peradilan, lop., cit, hlm 11-12.

memiliki keunggulan ketika setelah pengguna melakukan *reboot* komputernya, karena dapat menghapus data memori dengan kemampuan menyembunyikan diri, keuntungan lainnya dari *malware* dapat mengetahui kebiasaan dari korban selama jangka waktu tertentu. Serangan melalui *Open Source* menjadi serangan yang cukup banyak dilakukan oleh para pelaku kejahatan siber setelah *malware,* cara yang digunakan dengan mencari celah kelemahan para pengguna yang merasa kurang percaya dengan aplikasi pencarian/*open source*.[68]

Bentuk dari ancaman siber beragam dan banyak dijumpai juga terjadi di ruang siber, adapun bentuknya sebagai berikut:[69]

a. Serangan *Advanced Persistent Threats* (ATP), *Denial of Service* (DoS), dan *Distributed Denial of Service* (DDoS), bentuk ancaman siber ini sering dilakukan *overloading* kapasitas sistem dan mencegah pengguna yang sah untuk dapat mengakses dan menggunakan sistem atau sumber daya yang ditargetkan. Bentuk ancaman seperti ini bertujuan untuk mengganggu operasional sistem, dengan cara menghadapkan sistem pada permintaan akses dan proses yang jauh lebih besar dari yang bisa ditangani sistem. Akibatnya sistem menjadi terlalu sibuk dan *crash*, dan tidak dapat beroperasi. Dampak yang timbulkan cukup berbahaya bagi organisasi yang

[68] Muhamad Danuri dan Suharnawi, *Trens Cyber dan Teknologi Informasi di Indoensia,* Jurnal Infokam, Edisi XIII, No. 2 Septemeber 2017, hlm 58-59.

[69] Kementerian Pertahanan RI, *Pedoman Pertahanan SIber,* (MENHAN: Jakarta, 2014), hlm 7-11.

mengandalkan hampir sepenuhnya pada kemampuan internet guna menjalankan roda kegiatannya.

b. Serangan *Defacement*, serangan ini dilakukan penggantian atau modifikasi terhadap halaman web korban yang bertujuan isi dari halaman web korban berubah sesuai dengan motif penyerang.
c. Serangan *Phishing*, bentuk dari serangsn ini lebih kepada memberikan alamat website palsu dengan tampilan persis sama dengan website aslinya. Tujuannya adalah untuk mendapatkan informasi penting dan sensitive seperti username, password, dan lain-lain. Biasa kejadian yang terjadi dengan metode mendapatkan infromasi atau data rahasia /sensitive dengan menipu pemilik informasi/data tersebut sehingga secara tidak sengaja korban memberikan informasi/data rahasia miliknya.
d. Penyusupan siber, yang mendapat serangan sistem melalui identifikasi pengguna yang sah dan parameter koneksi yang ada pada sistem. Metode utama yang digunakan untuk mendapatkan akses ke dalam sistem sebagai berikut:
    1) Menebak sandi yang begitu jelas, seperti nama pengguna, nama pasangan atau anak, tanggal lahir atau berbagai hal yang penting yang berkaitan dnegan diri dan keluarganya, sangat mudah untuk ditebak dan dipecahkan.

2) *Account* yang tidak terlindungi. Pengguna kemungkinan melakukan kesalahan, dengan tidak memasang *password* atau dengan mudah memberikan password kepada orang lain.
3) Penipuan dan Rekayasa Sosial, semisal pelaku mengaku dan bertindak sebagai *administrator* dan meminta *password* dengan beberapa alasan teknis. Sebagian besar kasus pengguna akan mengungkapkan data mereka. Pelaku dapat menipu melalui telepon atau pesan elektronik. Kebanyakan pelaku tidak faham komputer, tetapi ternyata pelaku dapat memperoleh kunci sesuai dengan sistem yang mereka inginkan untuk ditembus.
4) Mendengarkan lalu lintas komunikasi data. Penyadap akan mendengarkan data yang tidak terenkripsi yang dikirimkan melalui jaringan melalui protokol komunikasi. Mereka beroperasi menggunakan PC dengan menganalisis data dalam transit di jaringan, kemudian mengektraksi password terenkripsi yang ditularkan oleh pengguna selama koneksi. Jika pelaku tidak bisa mengandalkan keterlibatan dari dalam organisasi dalam mendapatkan password secara langsung, maka dengan bantuan perangkat elektronik mereka dapat mencegatnya dari *protocol* komunikasi atau mengakses file yang berisi semua password.
5) *Trojan Horse*. Program mata-mata yang spesifik dan sangat berbahaya *(spyware)* secara diam-diam dapat merekam parameter yang digunakan untuk menghubungkannya ke sistem remote. Trojan adalah sebuah

program kecil yang umumnya pengganti dirinya untuk kode login yang meminta pengguna untuk menangkap atau memberikan identifikasi dan password, dengan keyakinan bahwa ia berada dalam lingkungan operasi normal, dimana sandi segera ditransmisikan ke server sebagai pesan anonim dari pelaku.

6) Sistem otentifikasi. Semua password pengguna harus disimpan pada sebuah server. Pelaku akan mengakses file yang menyimpan semua password user yang dienkripsi, untuk kemdian dibuka dengan utilitas yang tersedia pada jaringan.
7) *Cracking Password* Terinnkripsi. Bila pelaku atau *cracker* tahu algoritma *cypher*, maka bisa menguji semua pemutasi yang mungkin merupakan kunci untuk memecahkan password. Jenis serangan disebut *brute force*. Alternatif dari itu menggunakan kamus dalam menemukan password terenskripsi, dengan cara perbandingan berurut, bentuk kode password yang terdapat dalam kamus kriminal yang digunakan untuk menebak password terenskripsi.
8) Memata-matai. Biasanya dilakukan dengan merekam parameter koneksi mereka dengan menggunakan *software. Spyware* atau perangkat *multimedia*, seperti kamera video dan mikrofon, untuk menangkap informasi rahasia, seperti password.

Beberapa jenis ancaman siber menurut Mcdonnell dan Terry L. Sayers terdapat tiga jenis, yaitu:[70]

a. Ancaman Perangkat Keras *(Hardware Threat)*

   Ancaman yang muncul karena pemasangan peralatan tertentu berfungsi melakukan kegiatan tertentu dalam suatu sistem, sehingga peralatan tersebut sebagai gangguan terhadap sistem jaringan dan perangkat keras lainnya, semisal: *Jamming* dan *Network Intrusion*.

b. Ancaman Perangkat Lunak *(Software Threat)*

   Munculnya ancaman ini dikarenakan masuknya *software* tertentu dengan melakukan kegiatan seperti; Pencurian Informasi/Sistem *(Information/System Destrcution)*, manipulasi informasi *(Information Corruption),* dan lain sebagainya, ke dalam suatu sistem.

c. Ancaman Data/Informasi *(Data/Informasi Threat)*

   Timbulnya ancaman ini diakibatkan oleh penyebaran data/informasi tertentu dengan maksud tertentu, semisal: dilakukan untuk *Information Warfare* termasuk kegiatan propanganda.

Dari penjelasan diatas tentu bentuk dari kejahatan siber dikatakan sebagai kejahatan yang modern dimana dengan sistem komputer segala motif dan

[70] Ibid, hlm 12.

tujuan pelaku terhadap bentuk kejahatan dapat dilakukan dengan berbagai resiko ancaman yang muncul

C. Perlindungan Data Pribadi

1. Pengertian dan Konsep Data Pribadi

Data dalam konsep hukum telematika merupakan representasi formal suatu konsep, fakta atau intruksi. Data merupakan bentuk jamak dari datum, yang dari Bahasa Latin adalah "suatu yang diberikan". Pengertian Data diartikan sebagai setiap informasi melalui proses dengan peralatan yang berfungsi secara otomatis menanggapi instruksi-instruksi yang diberikan pada tujuannya dan disimpan dengan maksud untuk dapat diproses, termasuk bagian tertentu baik itu mengenai kesehatan, kerja sosial, pendidikan atau yang disimpan sebagai bagian dari suatu sistem penyimpanan.[71] Sedangkan informasi merupakan data yang diinterpretasikan dengan berbagai cara melalui prosedur dan alat bantu tertentu berdasarkan pada pengetahuan. Beberapa pendapat mengenai informasi salah satunya menurut Toto (2006) adalah informasi sebagai hasil dari proses pengolahan data yang disimpan, diproses dan disiarkan sebagai suatu pesan dalam bentuk yang lebih berguna dan berarti bagi penerimanya, agar menjadi suatu gambaran tentang kejadian nyata dan dapat dipergunakan sebagai pengambilan keputusan

[71] Tesis UI, hlm 18

Konsep privasi merupakan multidimensi, para pakar telah berupaya melakukan definisi yang tunggal agar mempermudah pemaknaan tentang privasi. Pada Esai Warren dan Brandeis mengenai hak privasi berdasarkan prinsip "kerpibadian yang tak terlanggar", yang dapat kita pahami sebagai kendali atas informasi sendiri,[72] salah satu karya tulis yang berjudul "*The Right to Privacy"* menjelaskan bahwa:[73]

> *"Privacy is the right to enjoy life and the right to be left alone and this development of the law was inevitable and demanded of legal recognition"*

Konsep mengenai privasi berawal dari gagasan menjaga integritas dan martabat pribadi itu sendiri, memang bila didefinisi sulit untuk menggambarkan dengan tepat pengertian privasi. Karena sangat berkaitan erat dengan pikiran dan hati nurani, baik dalam hal hak untuk menyendiri, hak untuk mengontrol tubuh sendiri, hak untuk melindungi reputasi diri sendiri, serta hak untuk kehidupan keluarga. Bila dikaitkan dengan perkembangan teknologi cakupan dan ruang lingkup tentang privasi sangat berkaitan dengan kemajuan teknologi pada masa tertentu, yang mana perkembangan teknologi itu sendiri berubah begitu cepat. Umumnya privasi yang diketahui berhubungan pada upaya membatasi pihak dari luar terhadap ruang fisik, dan

---

[72] Shraddha Kulhari, *Data Proctetion, Privacy, and Identity: A Complex Triad,* (Nomos Verlagsgesellschaft), hlm 23. https://www.jstor.org/stable/j.ctv941qz6.7

[73] Samuel Warren dan Louis D. Brandeis, *The Right To Privacy,* Hardvard Law Review ol. 4, 1890, hlm 1, dikutip dari buku Sinta Dewi Rosadi, *Cyber Law: Aspek Data Privasi Menurut Hukum Internasional, Regional, dan Nasional*, cetakan pertama, (Refika Aditama: Bandung, 2015), hlm 23.

perlindungan rumah dan barang-barang pribadi. Semula privasi berfokus pada tidak dapat diganggu-gugatnya kehidupan pribadi rumah tangga dan keluarga. Disisi lain sebagai upaya mengontrol informasi apa yang diketahui tentang seseorang dengan cara memanfaatkan teknologi. [74] Warren beranggapan bahwa privasi menjadi salah satu hak yang harus dilindungi dengan alasan bahwa:[75]

a. Manjalin hubungan dengan orang lain, maka seseorang harus membatasi sebagian kehidupan pribadinya agar dapat mempertahankan posisinya pada tingkat tertentu
b. Setiap orang perlu waktu untuk menyendiri *(solitude)*, sehingga privasi sangat dibutuhkan oleh seseorang
c. Privasi sebagai hak untuk menyendiri dan tidak bergantung kepada hak lain, tetapi hilang apabila orang tersebut mempublikasikan hal-hal yang bersifat privasi kepada umum
d. Privasi termasuk hak seseorang untuk dapat berhubungan *domestic* termasuk bagaimana seseorang membina perkawinan, keluarga dan orang lain tidak boleh mengetahui hubungan pribadi tersebut

[74] Wahyudi Djafar dan Asep Komarudin, *Perlindungan Hak Atas Privais di Internet; Beberapa Penjelasan Kunci,* cetakan pertama, (ELSAM: Jakarta, 2014), hlm 3.

[75] Sinta Dewi Rosadi, op.cit, hlm 24.

e. Pelanggaran privasi menimbulkan kerugian yang diderita dan sulit untuk dinilai. Kerugiannya dirasakan jauh lebih besar dibandingkan dengan kerugian secara fisik,

Melihat beberapa uraian diatas maka pembatasan terhadap privasi dibutuhkan dan tidak hanya dipandang sebagai pembatasan terhadap orang lain atas hak privasi seseorang untuk diketahui atau dipublikasi, termasuk menjalin hubungan antara hak-hak tertentu pada posisinya untuk dihargai dan dihormati, sehingga menimbulkan hubungan sosial yang bebas terbatas terhadap privasi setiap orang. Begitu pun sebaliknya bila privasi itu tidak menjadi suatu yang perlu dilindungi dan dibatasi tentu hilang kedudukan seseorang sebagai pribadi yang harus dihormati/dihargai.

Perlindungan data atau informasi secara khusus dijelaskan oleh Alan Wastin yang mendefiniskan pertama kali data privasi atau "*information privacy"* sebagai hak individu, keluarga ataupun kelompok sejauh mana mereka dapat menentukan hal-hal yang dibatasi atas data privasinya. Kemudian dikembangkan oleh pakar hukum lainnya, salah satunya Arthur Miller yang menjelaskan data privasi sebagai kemampuan seseorang dapat mengontrol informasi yang berkaitan pada dirinya dapat diketahui. Begitu juga dalam hal perkembangan teknologi tentang informasi seseorang yang dapat diakses, diproses, dikumpulkan dan dimanupulasi secara umum. Pandangan Westen juga atas hak privasi tidaklah absolut, sebab memiliki

konseksuensi sosial sebagai tanggungjawab yang perlu diperhatikan atas informasi privasi individu.[76]

Konsep hak privasi yang dijelaskan oleh Warren dan Brandeis juga mempertegas konsep privasi sebagai *"the right to be alone"*[77] yang menjadi dorongan konsep atas privasi dalam Pasal 12 Deklarasi Umum Hak Asasi Manusia terbentuk, bunyinya sebagai berikut:

> *"Tidak seorangpun dapat diganggu dengan sewenang-wenang urusan pribadi, keluarga, rumah tangga atau hubungan surat-menyurat, juga tak diperkenankan pelanggaran atas kehormatan dan nama baiknya. Setiap orang berhak mendapatkan perlindungan hukum terhadap gangguan atau pelanggaran seperti itu"*

Melalui *International Civil and Politiical Rights* (ICCPR) dipertegas dengan adanya Pasal 17 ICCPR yang diuaraikan dalam beberapa ayat:

> *"(1) Tidak boleh seorangpun yang dapat secara sewewang-wenang atau secara tidak sah mencampuri masalah-masalah pribadinya, kelaurganya, rumah atau hubungan surat-menyurat, atau secara tidak sah diserang kehormatan dan nama baiknya*
> *(2) Setiap orang berhak atas perlindungan hukum terhadap campur tangan atau serangan sepertu tersebut diatas"*

Melihat aspek hak atas akses dan kontrol data pribadi seseorang dengan media elektronik oleh Manfred Nowak kepada *Human Right Committee* (HRC) ditegaskan secara jelas dalam komentar Umum 16 ICCPR yang bunyinya:

---

[76] Wahyudi Djafar, Bernhard Ruben Fritz, dan Blandina Lintang, *Perlindungan Data Pribadi; Usulan Pelembagaan Kebijakan dari Perspektif HAM*, cetakan pertama, (Jakarta: ELSAM, 2016), hlm 5.

[77] Samuel I Warren and Louis D. Brandeis, *The Right to Privacy,* dikutip dalam Wahyudi Djafar etc, hlm 6.

> *"Pengumpulan dan penyimpanan informasi pribadi di komputer, bank data dan alat mekanik lainnya, baik oleh pihak berwenang publik atau individu-individu atau badan badan, harus diatur oleh hukum. Langkah-langkah yang efektif harus diambil oleh negara-negara guna menjamin bahwa informasi yang berkaitan dengan kehidupan pribadi seseorang tidak jatuh ke tangan orang-orang yang tidak memiliki kewenangan secara hukum untuk menerima, memproses dan menggunakannya, dan tidak boleh digunakan untuk tujuan-tujuan yang tidak sesuai dengan ICCPR. Guna mendapatkan perlindungan yang efektif bagi kehidupan pribadinya, setiap individu harus memiliki hak untuk menentukan data-data pribadi apa dan untuk tujuan apa yang akan disimpan dalam rekaman data otomatis. Jika rekaman data tersebut memuat data pribadi yang tidak benar atau dikumpulkan atau diproses dengan cara yang bertentangan dengan ketentuan-ketentuan hukum, maka setiap individu harus memiliki hak untuk meminta perbaikan atau pemusnahan data tersebut."*

Perlindungan hak privasi semata-mata bertujuan melindungi individu atas gangguan yang dianggap melanggar hukum dan tindakan lainnya yang sewenang-wenang terhadap informasi privasi, tetapi gambaran yang diberikan juga tidaklah cukup detail mengenai pengertian 'gangguan yang sewenang-wenang' atau 'melawan hukum' *(unlawfull interference)* terhadap privasi. Unsur-usnur yang dapat dilakukan tentunya telah ditetapkan oleh Undang-Undang sebagai gangguan yang telah memenuhi prasyarat yang ditentukan.[78]

2. Prinsip-prinsip Perlindungan Data Pribadi

Perlindungan atas data pribadi tentu harus memperhatikan bagaimana pelaksanaan semua kegiatan yang berkaitan baik dalam cara pemrosesan,

[78] Wahyudi Djafar dan Asep Komarudin, op.cit, hlm 6-7.

pengelolaan, penggunaan, penyebarluasan data pribadi, sehingga tidak lepas dari prinsip-prinsip yang mendasarinya seperti yang diatur dalam *APEC Privacy Framework* sebagia berikut:[79]

a) Pengumpulan data pribadi, disimpan, diproses atau digunakan secara *fair* dan *lawfully*. Cara mengetahui proses yang *fair* atau *unfair* dapat diketahui melalui metode cara memperloleh, menyimpan, memproses, atau menggunakan data tersebut. Perolehan data pribadi tentu untuk satu dan lebih maksud tertentu yang sah, dan pengecualian yang diperbolehkan hanya untuk maksud yang sah serta berkaitan langsung dengan suatu fungsi atau kegiatan pengelolaan dan menggunakan data tersebut dan data tersebut layak, relevan dan sesuai tujuan yang dimaksukan.
b) Penggunaan Data Pribadi, yang dikelola wajib dengan persetujuan subyek pemilik data, diperuntukan sesuai dengan yang dimaksud atau suatu tujuan yang langsung berkaitan dengan maksud tersebut. Data yang digunakan tidak diperbolehkan bila tidak sesuai dengan apa yang ditujukan.
c) Pengungkapan Data Pribadi, tidak diperboleh untuk digunkana tanpa melalui persetujuan dari subyek pemilik data, kecuali dengan maksud semula atau secara langsung berkaitan dengan maksud diperolehannya.
d) Keakurasian Data Pribadi, langkah-langkah secara praktis yang perlu diambil sebagai jaminan agar data pribadi akurat, lengkap, relevan, tidak

[79] Sinta Dewi, *Prinsip-prinsip Perlindungan Data Pribadi di Nasabah Kartu Kredit Mneurut Ketentuan Nasional dan Implementasinya,* Jurnal Sosiohumaniora, Vol. 19, No. 3 2017, hlm 209.

menyesatkan, serta *update*, dengan melihat maksud cara memperolehan dan pengunaan data tersebut.

e) Jangka Waktu Penyimpanan Data Pribadi, proses penyimpanan sebagai maksud untuk tidak boleh disimpan dalam jangka waktu lama dari waktu yang diperlukan. Secara tegas prinsip ini bertujuan agar pengelola data me-*review* data tersbeut secara konsisten dan teratur, serta bila sudah tidak diperlukan lagi dapat dihapus, kecuali diperlukan untuk kepentingan umum.

f) Akses dan Koreksi terhadap Data Pribadi, pemilik dari data tersebut memiliki hak akses atas data pribadinya yang mana dikelola oleh pihak pengelola data, dengan tujuan dapat melakukan koreksi dan cek sehubungan dengan data pribadinya.

g) Keamanan Data Pribadi, keseluruhan langkah yang harus ditempuh oleh pihak pengelola data untuk mencegah akses data, pemrosesan data, perubahan data, pengungkapan data serta kerusakan yang secara melawan hukum termasuk suatu tindakan yang dapat merugikan pemilik data pribadi. Perhatian terhadap hal-hal yang perlu dicermati oleh pihak pengelola data terbeut harus melihat; sifat dan ancaman atas data pribadi, lokasi dimana data tersebut disimpan, penggunanan sistem keamanan, mitigasi untuk menjamin kehandalan, integritas dan kompetensi individu dalam mengakses ke data, dan tindakan sebagai jaminan transmisi aman atas data tersebut

h) Informasi Secara Umum yang Tersedia, keterkaitan pengelolaan data harus memformulasikan kebijakan dan implementasi dalam pengelolaan dan pemrosesan data, yang harus ditempuh sebagai langkah yang dipandang perlu agar subyek data memperoleh informasi mengenai beragam data yang disimpan oleh pihak pengelola data.

Terobosan yang menjadi rumusan dalam kerangka kerja privasi APEC atau yang dikenal *APEC Privacy Framework* penting sebagai pembangunan perlindungan data privasi atas data pribadi. Terutama indikasi dampak negatif yang muncul dari kebocoran data, tidak ada izin dan penyalahgunaan data pribadi, serta komitmen dari APEC atas kebebasan arus informasi yang sangat fundamental pada setiap individu.[80]

3. Klasifikasi Data Pribadi

Data pribadi secara sederhana merupakan gambaran mengenai individu, atau semua data tentang orang perseorangan yang teridentifiasi secara sendiri atau kombinasi dengan informasi lainnya. Bila dilihat secara detail tentu data pribadi dapat dibagi dalam beberapa hal baik yang berupa data yang dapat diakses secara publik dan data spesifik *(sensitive)*.

Pada beberapa negara yang telah mengatur regulasi mengenai perlindungan data pribadi secara rinci juga memisahkan data yang dapat diakses secara

[80] Wahyudi Djafar, et. al, op. cit., hlm 9-10.

publik dan data yang bersifat sensitif, seperti Inggris diatur dalam *Data Procettion Act* 1998 (DPA), memberikan gambaran mengenai data sensitif sebagai data seseorang yang memuat unsur informasi berkaitan:[81]

a) Identitas rasa tau etnis
b) Pandangan politik
c) Keyakinan beragama atau kepercayaan
d) Keanggotaan dlaam suatu serikat kerja
e) Kondisi kesehatan fisik atau mental
f) Kehidupan seksual dan,
g) Catatan kriminal individu

Bahkan di Uni Eropa juga telah mangatur perlindungan data pribadi dan telah lebih merincikan klasifikasi data yang dapat di akses, sebagai berikut:[82]

a) Bukan Data Pribadi: alamat anonim, alamat email yang umum (seperti info@HelpIT.com), resi dengan data, waktu, 4 angka terakhir pada nomor credit card dan tanpa nama atau alamat email, akun perusahaan dengan ringksan data gaji, dan perushaan dan alamat website.
b) Data Pribadi: nama dan alamat email pribadi, nama berserta 4 angka terakhir pada credit card, dan web cookie.

[81] Ibid, hlm 15

[82] Djafar Wahyudi, Seminar Online, *Perlindungan Data Pribadi dalam Pengelolaan Data Bantuan Sosial,* hlm 7

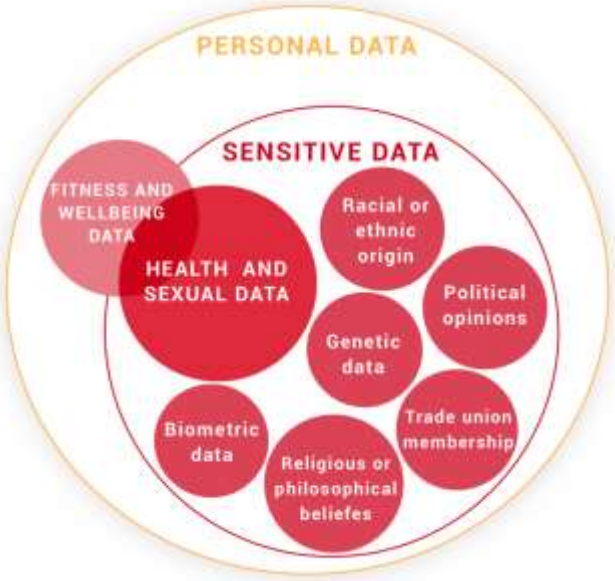
c) Data Pribadi Spesifik *(sensitive)*: ras atau etnis tertentu, pandangan politik, agama dan kepercayaan, seksual preferensi, dan informasi biometric.

Indonesia juga sedang membahas mengenai Rancangan Undang-Undang Perlindungan Data Pribadi (RUU PDP) yang mana dalam RUU PDP juga memisahkan antara data pribadi yang bersifat umum dan bersifat privat, penjelasan mengenai data privat terdapat pada Pasal 3 RUU PDP, sebagai berikut:[83]

a) Data dan informasi kesehatan
b) Data biometric
c) Data genetik
d) Orientasi seksual (termasuk jenis kelamni)
e) Pandangan politik
f) Catatan kriminal
g) Data anak
h) Data keuangan pribadi

[83] Sih Yuliana Wahyuningtyas, Webniar Online, *Beberapa Catatan RUU PDP dan Aktualitas Menjawab Tantangan*, hlm 7

Bila dibuat tabel diagram yang dilakukan oleh Peneliti Lembaga Studi dan Advokasi Masyarakat menunjukkan persinggungan antara data pribadi dan data sensitif, sebagai berikut:[84]



Gambar 1.1

Data pribadi telah menjadi industri baru di ruang siber, yang mana untuk mengembangkan suatu bisnis di dunia digital yang didapat di ruang siber untuk membantu dalam melihat kebutuhan dan peluang dari konsumen yang dapat menghasilkan keuntungan dari data pribadi yang diperoleh, tanpa memperhatikan kerugian yang secara tidak langsung dapat menimbulkan kerugian bagi pemilik data pribadi.

[84] Lintang, *The Future; Personal Data Must Be Protected,* seminar online

BAB III

PEMBAHASAN DAN ANALISA

A. Kemampuan Hukum Pidana Pada Undang-Undang Informasi dan Transaksi Elektronik Dalam Menanggulangi Kejahatan Siber Terkait Perlindungan Data Pribadi

Tindak pidana dalam beberapa literatur sering disebut sebagai ‘delik’ atau perbuatan pidana, ketika berbicara mengenai perbuatan dan jenis-jenis delik sama halnya kita berbicara mengenai unsur-unsur perbuatan pidana dan jenis-jenis perbuatan pidana.[85] Merujuk pada istilah perbuatan yang dilarang dan diancam pidana banyak ahli hukum menggunakan istilah yang berbeda, Moeljatno menggunakan perbuatan pidana untuk mendefinisikan perbuatan yang dilarang oleh hukum, serta adanya sanksi yang diberikan bila melanggar ketentuan tersebut. Berbeda dengan Sudarto yang menyebutnya dengan tindak pidana dengan pertimbangan bahwa tindak pidana lebih lazim dan dikenal dalam pembentukan undang-undang yang telah terdapat di berbagai perundang-undangan, secara sosiologis pun tindak pidana dapat diterima dan telah mempunyai keberlakuan *(sociologische gelding)* oleh masyarakat. Begitu juga Roeslan Saleh dan Oemar Seno Adji yang memilih menggunakan istilah perbuatan pidana dan istilah delik.[86]

[85] Eddy O. S. Hiariej, *Prinsip-prinsip Hukum Pidana,* cetakan kelima, (Cahaya Atma Pustaka, Yogyakarta, 2016) ,hlm 129

[86] Sudaryono dan Natangsa Surbakti, *Hukum Pidana; Dasar-dasar Hukum Pidana Berdasarkan KUHP dan RUU KUHP,* tanpa cetakan, (Muhammadiyah University Press: Surakarta, 2017), hlm 92

Dari penjelasan para ahli hukum mengenai delik sejatinya merujuk pada suatu perbuatan atau peristiwa hukum yang mana untuk memberi gambaran apa yang menjadi unsur-unsur dari suatu tindak pidana, sehingga dalam implementasi mengenai suatu perbuatan pidana dapat secara tepat diterapkan.

Pengaturan terkait kejahatan siber haruslah dilihat mengenai tindak pidananya, unsur-unsur dari tindak pidananya dan delik yang dirumuskan dalam suatu perundang-undangan, serta ancaman sanksi yang diberikan. Kebijakan dalam memformulasi tindak pidananya bila tidak merefleksikan hal tersebut tentu dapat meruntuhkan kepercayaan terhadap sistem peradilan yang dianggap tidak adil.[87] Hal tersebut akan mempengaruhi pada penjatuhan pidana oleh hakim yang kemungkinan dalam menjatuhkan sanksi yang diberikan tidak adil.[88]

Tindakan atas pelanggaran terhadap data pribadi bila mengacu pada instrumen hukum Internasional mengenai Hak Asasi merupakan entitas dalam penghormatan atas hak setiap individu. Pada Pasal 12 Deklarasi Universal HAM dan Pasal 17 Kovenan Internasional Hak-hak Sipil dan Politik, menyebutkan perlindungan hukum atas hak setiap orang terhadap intervensi dan serangan dari pihak lain yang dianggap dapat mengganggu privasi seseorang. Dalam hal ini tentu data pribadi menjadi hak fundamental yang melekat pada setiap orang yang harus dilindungi

[87] Mahrus Ali, *Proposional dalam Kebijakan Formulasi Sanksi Pidana,* Jurnal Hukum IUS QUIA IUSTUM, Vol 25, No. 1, 2018, hlm 158.

[88] Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan,* cetakan ketiga, (Kencana Prenada Group; Jakarta, 2010), hlm 2

tanpa ada pengawasan yang sewenang-wenang. Sehingga terhadap semua akses yang memanfaatkan teknologi mengenai data pribadi harus dinyatakan secara jelas bentuk dan sifatnya agar tidak berdampak merugikan pemilik data.

Pengakuan atas hak privasi dalam Undang-Undang HAM[89] di Indonesia juga mengakui perlindungan atas diri pribadi, keluarga, kehormatan, dan hak miliknya. Indikasi pertukaran informasi atas data pribadi dengan mamanfaatkan teknologi, tidak menutup kemungkinan hal tersebut digunakan tanpa adanya ijin. Hal tersebut diatur juga dalam Pasal 14 ayat (2) mengenai salah satu hak berupa mengembangkan diri dengan mancari, memperoleh, menyimpan, mengolah, dan menyampaikan informasi pribadi seseorang secara tidak sah dan menggunakan segala jenis sarana yang digunakan. Pasal tersebut memberikan jamin akan kemerdekaan dan kerahasiaan dalam berkomunikasi melalui sarana elektronik.

Ketentuan mengenai informasi data pribadi di Indoenseia masih diatur secara parsial dan telah banyak disebutkan dibeberapa Undang-Undang sektoral yang mengatur mengenai kerahasian infomasi/data pribadi. Setidaknya ada 32 undang-undang yang materinya berkaitan dengan pengaturan data pribadi, mulai dari sektor keuangan, perpajakan, keamanan, kependudukan, kearsipan, penegakan hukum telekomunikasi, perbankan sampai pada sektor kesehatan.[90] Penulis akan

[89] Pasal 29 ayat (1) Undang-Undang Nomor 39 Tahun 1999 Tentang Hak Asasi Manusia

[90] ELSAM, "UU Perlindungan Data Pribadi Segara DIwujudkan", https://elsam.or.id/ruu-perlindungan-data-pribadi-penting-menjadi-prioritas-prolegnas-2019/, diakses pada 30 November 2020.

menjelaskan beberapa Undang-Undang yang terkait dengan data pribadi yang berpengaruh terhadap pemanfaatan teknologi. Di sektor perbankan misalnya, privasi atas pengguna bank dilindungi yang diatur perihal rahasia bank[91]. Pemilik dari data pribadi disebut sebagai nasabah dalam hal melakukan penyimpanan atau menggunakan produk bank. Nasabah diwajibkan untuk memberikan data pribadi yang dibutuhkan pihak bank, sebagai timbal balik dari bank untuk melindungi data nasabah tentunya wajib menjaga data yang diberikan oleh nasabah. Berdasarkan asas kepercayaan dan kerahasiaan bank wajib menjaga data milik nasabah, tetapi hal tersebut dapat dikecualikan dalam hal tertentu yang diperbolehkan oleh undang-undang. Ketentuan tersebut tidak hanya melindungi data nasabah yang berkaitan dengan keuangannya saja tetapi juga termasuk informasi yang bersifat identittas menyangkut nasabah atau data diluar data keuangan.[92]

Pada Undang-Undang Keterbukaan Infomasi Publik[93] memang tidak secara eksplisit mencantukan berkaitan dengan data pribadi, tetapi secara tidak lanngsung definisi mengenai Informasi mengarah pada Informasi pribadi termasuk data pribadi.[94] Pada Pasal 6 ayat (3) terdapat informasi yang tidak boleh diberikan kepada

[91] Pasal 1 ayat (28) berbunyi bahwa segala sesuatu yang berhubungan dengan keterangan mengenai nasabah penyimpanan dan simpanananya

[92] Sugeng, *Hukum Telematika Indonesia,* cetakan pertama, (Kencana; Jakarta, 2020), hlm 69.

[93] Undang-Undang Nomor 14 Tahun 2008 Keterbukaan Informasi Publik.

[94] Pasal 1 ayat (1) Undang-Undang Keterbukaan Informasi Publik berbunyi "bahwa informasi adalah keterangan, pernyataan, gagasan, dan tanda-tanda yang mengandung nilai, makna, dan pesan baik data, fakta maupun penjeleaannya yang dapat dilihat, didengar, dan dibaca yang disajikan dalam berbagai kemasan dan format sesuai dengan perkembangan teknologi informasi dan komunikasi secara elektronik/non-elektronik.

publik atas dasar perlindungan data dan informasi yang dihimpun oleh badan publik, yaitu:

1. Informasi yang membahayakan negara
2. Informasi berkaitan dengan kepentingan perlindungan usaha dari persaingan tidak sehat
3. Informasi berkaitan dengan hak-hak pribadi
4. Informasi berkaitan dengan rahasia jabatan
5. Informasi publik yang diminta belum dikuasai atau didokumentasikan

Lebih dipertegas lagi dalam Pasal 17 huruf h menjelaskan mengenai infomasi yang dapat mengungkapkan tentang riwayat dan kondisi anggota keluarga, kondisi dan perawatan yang berkaitan dengan kesehatan baik fisik maupun psikis seseorang, pendapatan dan kondisi keuangan, serta catatan menyangkut dengan kegiatan pendidikan formal dan non-formal. Pertimbangan atas hal tersebut dianggap dapat merugikan pihak tertentu apabila informasi tersebut diketahui oleh publik. Keterbukaan Informasi dan data pribadi keduanya juga penting untuk dijaga terutama dalam hal infromasi digital di era saat ini, dan pemerintah juga tetap bertanggungjawab terhadap warganya atas kedua hal tersebut.

Begitu juga dalam Undang-Undang tentang Kesehatan[95] yang berkiatan dengan perlindungan mengenai riwayat kesehatan pasien yang dianggap sebagai data

[95] Undang-Undang Nomor 36 Tahun 2009 Tentang Kesehatan.

pribadi yang harus dijaga, dengan menyebutkan atas hak setiap orang terhadap kerahasiaan kondisi kesehatan pribadinya, dan terdapat beberapa pengecualian yang secara terbatas diperbolehkan dalam Undang-Undang ini. Meskipun adanya pengakuan hak pasien untuk mendapatkan perlindungan atas riwayat kesehatannya, tetapi perlindungan data pribadi pasien tidak semuanya mencakup dalam Undang-Undang tersebut.[96]

Jika melihat pengaturan terkait dengan penyelenggaraan negara yang berkaitan dengan Administrasi Pemerintahan, mengatur perihal data pribadi pada Pasal 1 angka 22 [97]yang dalam pasal tersebut telah diamanatkan perlindungan kerahasiaan dari data pribadi. Lebih dipertegas juga dalam pasal 79 ayat (1) dan Pasal 85 ayat (3) mengenai data dan dokumen kependudukan yang wajib disimpan dan dilindungi oleh negara, serta dijaga kebenarannya dan dilindungi kerahasiaannya oleh penyelenggara dan instansi. Sama halnya dengan Pasal 51 Undang-Undang tentang Administrasi Pemerintahan[98] yang menjelaskan untuk hak mengakses dokumen Administrasi Pemerintahan tidak dapat diberlakukan yang berkaitan dengan rahasia negara dan/atau melanggar kerahasiaan pihak ketiga, yang dimaksud pihak ketiga disini ialah setiap data dan informasi pribadi seseorang.

[96] Sugeng, op. cit., hlm 75-76.

[97] Pasal 1 angka 22 berbunyi Data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya.

[98] Undang-Undang Nomor 30 Tahun 2014 Tentang Administrasi Pemerintahan.

Dari penjelasan diatas, maka kejahatan atas data pribadi seseorang yang tercantum di berbagai Undang-Undang berbeda bila terjadi di ruang siber, yang mana mneggunakan pemanfaatan teknologi sebagai sarana untuk mendapatkan data pribadi yang bersifat elektronik.

Pergeseran data atau informasi seseorang yang beralih dengan memanfaatkan teknologi menjadikan Indonesia memerlukan peraturan yang setidaknya dapat menjadi payung hukum *(lex specialis derogat legi generali)* dalam mengatur penggunaan, pengumpulan, penyebarluasan dan pelanggaran yang patut dikriminaliasaikan, serta dianggap dapat merugikan masyarakat dan negara. Pelanggaran atas data pribadi di dunia siber merupakan kejahatan yang dikatakan sebagai *cyber related crime*. Ciri khusus *cyber related crime* yaitu luasnya konsep dan pemahaman kejahatan *offline* yang disebut menjadi kejahatan siber yang saat kejahatan dilakukan dengan melalui media komputer atau internet. Isitilah ini berkaitan dengan tindakan yang sebenarnya dilarang oleh undang-undang dengan memanfaatkan penggunaan teknologi digital, semisal *revenge pron, cyber pornography, identity theft, cyber harassment* dan *skinning*. Kejahatan yang disebutkan sebenarnya telah ada di masyarakat hanya saja tanpa menggunakan bantuan perangkat elektronik atau ruang siber, sehingga *cyber related crime* hanya memberikan ruang yang berbeda atas perkembangan teknologi. Sedangkan kejahatan siber *(cybecrime)* sebagai kejahatan yang hanya dapat dilakukan dengan menggunakan komputer atau jaringan, atau secara sederhananya kejahatan yang

media utamanya dalam tindak kejahatan adalah komputer yang di dalamnya berupa kejahatan misalnya penyebaran virus, *malware*, *spyware, hacking atau DDoS* seperti dalam BAB sebelumnya telah dijelaskan.[99] Selain itu sebagai jaminan pemenuhan atas perlindungan data pribadi dan menjadikan pihak penyelenggara sistem elektronik yang tidak relevan dapat dikendalikan atas permintaan pemilik data.

Secara umum konsep mempresepsikan hukum di bidang pemanfaatan teknologi ada tiga aliran, yaitu:[100]

1. Separatisme: menghendaki setiap sektor diatur secara khusus dalam peraturan yang terpisah (dikehendaki umumnya oleh kalangan IT)
2. Internasionalisme: menghendaki segala konvensi internasional diadopsi di Indonesia
3. Negaraisme: menghendaki segala sesuatunya harus diatur pada aturan formal.

Melihat atas kejahatan dengan pemanfaatan teknologi, ketentuan mengenai peraturan kejahatan teknologi dibuat secara khusus, sebagai acuan dalam merumuskan hal tersebut juga mengacu pada konvensi internasional mengenai kejahatan teknologi, juga melihat norma yang ada di masyarakat, dan diundangkan dengan undang-undang tersendiri (diluar KUHP).

---

[99] Iftah Putri Nurdiani, *Pencurian Identitas Digital Sebagai Bentuk Cyber Related Crime,* Jurnal Kriminologi Indonesia, Vol. 16, No. 2 November 2020, hlm 3.

[100] Al. Wisnubroto, *Konsep Hukum Pidana Telematika,* cetakan pertama, (Yogyakarta: Universitas Atma Jaya, 2011), hlm 116.

Materi dari Undang-Undang Infromasi dan Transaksi Elektronik (Undang-Undang ITE) untuk menjangkau perkembangan elektronik meliputi tentang informasi dan dokumen elektronik, pengiriman dan penerimaan surat elektronik, tanda tangan elektronik, transaksi elektronik, hak atas kekayaan intelektual dan data privasi elektronik dengan pemanfataan teknologi.[101] Peraturan mengenai pemanfaatam teknologi yang berkaitan dengan data atau informasi bersifat elektronik telah diatur dalam Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Pada Undang-Undang ITE memang disebutkan terkait dengan data pribadi tetapi tidak menjelaskan definisi mengenai data pribadi dan belum memuat aturan perlindungan data pribadi secara jelas, tetapi hanya menyebutkan dalam pemanfaatan teknologi dan informasi mengenai data pribadi merupakan salah satu bagian dari hak pribadi *(privacy rights)* yang mana hak pribadi untuk menikmati kehidupan pribadi dan bebas dari segala gangguan, berkomunikasi dengan orang lain tanpa ada intervensi dari pihak manapun, dan hak untuk mengawasi dan mengakses data pribadinya. Sayangnya pengaturan yang merupakan aturan pelaksana yang lebih menjelaskan secara detail mengenai Penyelenggara Sistem Transaksi Elektronik (PSTE) mengenai data pribadi yang diatur dalam Peraturan Menteri (Permen) tersebut, lebih memberikan definisi data pribadi bahwa data peorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta

[101] Widodo, op,. cit. hlm 49.

dilindungi kerahaisaannya. Artinya Undang-Undang ITE yang sekarang menjadi peraturan tersendiri hanya berfokus pada pengaturan sektor informasi eletronik dan transaksi eletronik, sedangkan mengenai hal lain yang berkaitan dengan hal lebih khusus diatur secara terpisah atau lebih khusus. Sebenarnya yang dimaksud dengan informasi yang bersifat elektronik dapat dilihat pada ketentuan umum Pasal 1 ayat (1) Undang-Undang ITE yang memberikan definisi mengenai Informasi elektronik yakni:

"satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, electronic data interchange (EDI), surat elektronik (electronic mail), telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya".

Berkaitan dengan data pribadi, pada penjelasan di atas bahwa data yang sifatnya elektronik juga dapat dimasukan dalam bagian informasi elektronik, yang mana dijelaskan tidak hanya terbatas pada hal-hal yang disebutkan dalam Pasal tersebut, tetapi data yang bersifat elektronik juga dalam hal tersebut bisa dipahami oleh orang yang mengetahui sebagai informasi elektronik.

Indonesia sendiri sebenarnya telah mengadopsi pedoman yang dikeluarkan oleh OECD *(Organisation for Economic Co-operation and Development*) sebagai pedoman dalam menerapkan penegakan hukum atas privasi dan perlindungan data pribadi, sebagai anggota APEC dimana Indonesia termasuk dalam keanggotaannya juga telah mengikuti kerangka privasi APEC 2004 *(APEC Privacy Framework)*

sebagai acuan dalam membuat regulasi yang mengatur tentang perlindungan terhadap data pribadi.

Upaya penegakan hukum terhadap tindak kejahatan dengan pemanfaatan teknologi terkait data pribadi dengan menggunakan sarana penal dibutuhkan kajian terhadap materi substansi *(legal substance reform)*, mengingat kejahatan tersebut juga dianggap sebagai kejahatan *non- violence crime* yang menyebabkan korban tidak kasat mata.[102] Upaya dalam penanggulangan terhadap tindak kejahatan tersebut juga perlu diperhatikan mengenai kejahatan yang akan datang, serta pengaplikasiannya dalam merumuskan pada tataran aplikatif oleh para penegak hukum.[103]

Penentuan terhadap tindak pidana yang dirumuskan tentu perlu beberapa pertimbangan sebagai berikut: [104]

1. Memformulasikan suatu kejahatan dengan pemanfaatan teknologi tentu harus memilih dan menetapkan delik secara selektif dan limitatif, artinya penentuannya harus benar-benar dianggap sebagai kejahatan yang tidak dikehendaki dan tindakan yang menyimpang oleh masyarakat, serta dampaknya pun berpotensi merugikan dan mendatangkan korban, sebab kejahatan dengan pemanfaatan teknologi ini terjadi di ruang (siber) yang berbeda. Disisi lain juga harus melihat perkembangan nilai-nilai yang ada dalam masyarakat.

[102] Abdul Wahid dan Mohammad Labib, op.,cit, hlm 79.

[103] Yasmirah Mandasari S dan Dudung Abdul, *Perlindungan Data Elektronik Dalam Formulasi Kebijakan Kriminal Di Era Globalisasi,* Jurnal Soumatera Law Review, Vol. 3, No. 2, 2020, hlm 276.

[104] Al. Wisnubroto, op. cit., hlm 415.

2. Pertimbangan mengenai biaya *(cost)* yang dikeluarkan baik dalam hal penindakan/pengusutan terhadap kejahatan yang rumit dan kompleks, pengawasan, dan penegakan hukum melalui sarana dan prasarana dengan teknologi yang mumpuni, begitu juga dampak yang dialami oleh korban. Sehingga tindakan yang dilakukan dapat terjadi keseimbangan antara hasil dengan mengarah pada keadaan yang tertib hukum.
3. Kemampuan baik dari segi kualitas dan kuantitas para penegak hukum terhadap daya kerjanya. Semisal berkaitan dengan tingkat pendidikan yang berdasarkan kemampuan *(skill)*, profesionalisme, pengalaman yang berkorelasi pada karakteristik penggunaan teknologi dalam tindak kejahatan, teknik dan teknologi yang digunakan.
4. Pertimbangan pengaruh sosial akibat kejahatan yang terjadi dengan pemanfaatan teknologi dalam hal bagaimana pengaruh pengkriminalisasi terhadap pelaku atau khususnya sikap pelaku dan masyarakat pada umumnya.

Penentuan terhadap kejahatan tersebut memilliki dimensi tersendiri yang mana ruang siber berbeda dan menentukan bahwa perbuatan itu sebagai sebuah bentuk kejahatan, oleh sebab itu penentuan terhadap tindak pidana tentu harus secara hati-hati dan harus tepat agar tidak menimbulkan kerancuan dalam interpretasi hukum pada tataran aplikasi serta dapat diterapkan. Batasan suatu perbuatan atas tindakan perolehan dan pemanfaatan semua jenis data pribadi yang dikelola oleh pihak penyelenggara sistem elektronik pun harus memberikan klasifikasi. Sehingga

pengawasan terhadap data pribadi dapat secara jelas penentuan data yang diperbolehkan. Dalam hal ini kejahatan yang dilakukan di ruang siber pun membutuhkan pengawasan dari pihak yang berwenang dan bila terjadi suatu perbuatan kejahatan berkaitan dengan data pribadi juga harus mempertimbangkan antara dampak yang timbul serta upaya-upaya dalam pengusutan dan penyelesaian terhadap perbuatan tersebut dalam memberikan keseimbangan antara upaya yang telah dilakukan dengan hasil yang dicapai.

Penggungkapan terhadap kejahatan dengan pemanfaatan teknologi di ruang siber tentunya harus memiliki kemampuan yang kompeten dalam mengelola sistem komputer atau alogaritma dari perangkat teknologi tersebut. Sebab diperlukan keahlian khusus dari penegak hukum dalam penggungkapan kejahatan di ruang siber karena menjadi tantangan bagi penegak hukum pada kerumitan dan kompleks dari sistem teknologi yang ada dan perkembangan yang akan datang, tidak hanya itu sarana dan prasarana juga diperlukan sebagai bentuk memfasilitasi dan penelitian terhadap perkembangan dan tren kejahatan yang terjadi di ruang siber. Kemampuan dan fasilitas yang digunakan sebagai bentuk penyelesaian terhadap sebuah kejahatan sangat mempengaruhi citra dari penegak hukum yang professional dan handal. Bahkan upaya preventif dan mitigasi bila ada indikasi dapat dihindari.

Pencurian data pribadi *(identity theft)* juga dianggap sebagai kejahatan yang dianggap berpotensi dapat merugikan masyarakat dengan sarana pemanfaatan teknologi dirasa sebagai suatu kejahatan, sebab terjadi kelalaian atau adanya

pencurian terhadap data pribadi oleh pihak lain yang tidak memiliki tujuan dan tidak mempunyai otoritas yang patut dipertanggungjawabkan. Walaupun dalam hal ini telah diatur dalam Undang-Undang ITE tetapi bentuk dari suatu pasal mengenai hal tersebut lebih kepada ganti kerugian, padahal bila melihat peristiwa yang terjadi selama ini mengenai hal tersebut yang mengalami kerugian tidaklah beberapa orang saja bisa mencapai sampai dengan ratusan bahkan lebih dari itu data pribadinya yang telah diambil tanpa adanya ijin dari pemilik data tersebut.[105]

Optimaliasasi dari penegakan hukum atas kejahatan siber berkaitan dengan privasi seseorang pun harus melihat bagaimana peraturan tersebut memberikan solusi dalam penyelesaian terhadap pelaku kejahatan tersebut. Sehingga dalam konteks memberikan perlindungan dan kepastian hukum terhadap pengguna perangkat digital terhadap data pribadinya dapat terlindungi. Begitu juga melihat perilaku sosial di masyarakat atas pengkriminalisasi suatu perbuatan dan pandangan masyarakat terhadap bentuk dari tindakan yang dikriminalisasikan.

Bentuk perlindungan data pribadi dalam Undang-Undang ITE sebenarnya telah memuat bagaimana perlindungan yang diberikan kepada setiap orang, badan hukum, dan pemerintah, yang secara tegas melarang adanya akses secara melawan hukum terhadap informasi atau data milik orang lain melalui sistem elektronik untuk memperoleh suatu informasi dengan cara menerobos sistem pengamanan. Bentuk

[105] https://tekno.kompas.com/read/2020/05/05/19080067/kasus-kebocoran-data-di-indonesia-dan-nasib-uu-perlindungan-data-pribadi?page=all. Diakses pada tanggal 14 Desember 2020

lain yang secara gamblang disebutkan yaitu mengenai penyadapan *(interception)*, perbuatan penyadapan dilarang dengan pengecualian bila dilakukan oleh pihak yang memiliki otoritas dalam rangka penegakan hukum, serta gangguan terhadap data komputer. Undang-Undang ITE juga melarang setiap orang dengan cara apapun dengan memanfaatkan teknologi untuk mendapatkan suatu informasi milik orang lain dengan tanpa persetujuan pemilik data yang sifatnya rahasia sampai dapat terbuka ke publik.[106]

Ketentuan yang diatur dalam Undang-Undang ITE terhadap orang atau pihak yang merupakan pelaku kejahatan terhadap data pribadi dengan mengakses tanpa izin atau tanpa persetujuan atas data orang lain diatur pada Pasal 30 Undang-Undang ITE yang menyebutkan:

(1)*Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun.*
(2)*Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.*
(3)*Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.*

Terkaitan penjatuhan sanksi dalam Pasal 46 Undang-Undang ITE berbunyi:

(1)Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 600.000.000,00 (enam ratus juta rupiah).

[106] Asa Intan Primanta, *Pertanggungjawaban Pidana pada Penyelahgunaan Data Pribadi*, Jurnal Jurist-Diction, Vol. 3, No. 4 Juli 2020, hlm 1444.

(2)Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp 700.000.000,00 (tujuh ratus juta rupiah).
(3)Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (3) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp 800.000.000,00 (delapan ratus juta rupiah).

Melihat dari unsur Pasal di atas terhadap data yang bersifat elektronik melalui cara dengan mengakses data yang ada di dalamnya dengan tidak sah dapat diberlakukan dengan penerapan pasal ini sebagai tindakan akses yang tidak sah (*illegal access).* Sistem keamanan yang dimaksud bertujuan membatasi dengan klasifikasi atau kategorisasi pengguna serta tingkat kewenangan yang dimiliki. Bila mengacu pada ketentuan umum pada Undang-Undang ITE mengenai informasi elektronik juga berupa data yang tidak hanya terbatas pada tulisan, gambar, dan yang sudah dijelaskan pada Pasal 1. Ciri utama apakah data tersebut merupakan akses publik atau bukan dapat dilihat dari ada atau tidaknya suatu pengamanan sistem atau jaringan komputernya baik itu bisa berupa *password* atau kode akses. Menurut pendapat Agus Raharjo memasuki sistem atau jaringan komputer tersebut dengan memanfaatkan program Bahasa pemograman, yang mana ada pengungkapan kode Bahasa tertentu.[107] Sehingga setiap data yang dapat diakses dengan tanpa menggunakan kode akses berarti data tersebut difungsikan sebagai akses publik. Pengertian akses sendiri dipahami sebagai memasuki sistem komputer, meliputi perangkat keras, komponen, data penyimpanan dalam sistem

[107] Agus Raharjo, *Cybercrime: Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi,* cetakan pertama, (Citra Adhitya Bakti, Bandung, 2002), hlm 179-180.

peng-instal-an, direktori, dan lalu lintas data baik sebagain maupun keseluruhan, tidak hanya itu aktifitas akses yang dilakukan dengan memasuki sistem komputer, baik yang terhubung melalui sistem komputer. Cakupan dari pengertian akses tidak meliputi proses penerimaan surat elektronik (email) atau file dari suatu komputer ke komputer lain atau jaringan komputer serta berkomunikasi dengan bentuk komunikasi jarak jauh maupun dekat dengan atau tanpa kabel bukan merupakan pengertian akses. Perbuatan tersebut dalam beberapa negara sering diistilahkan termasuk memasuki jaringan komputer dengan akses tidak sah atau pelakunya disebut *hacking.*[108]

Akses yang tidak sah baik sengaja atau tidak disengaja pada sistem atau jaringan komputer milik orang lain yang dilindungi dengan kode akses maka dianggap sudah melanggar privasi pemilik sistem atau jaringan, sebab perbuatan terhadap akses yang tidak sah merupakan langkah awal dari perbuatan yang mengarah pada bentuk-bentuk kejahatan siber lainnya.

Istilah illegal akses bila melihat dari *Convention on Cybercrime* yang mana sebagai acuan umum terhadap kejahatan siber yang dibuat oleh Uni Eropa yang perkembangannya diratifikasi oleh berbagai negara sebagai tujuan upaya mengatasi kejahatan siber, memberikan penjelasan mengenai akses tidak sah *(illegal accees),* dalam *article 44 Convention on Cybercrime*, menjelaskan bahwa "*illegal access"*

[108] Widodo, op,. cit, hlm 67-70.

merupakan pelanggaran yang berbahaya dan serangan yang ditujukan pada keamanan sistem komputer dan data elektronik. Disamping itu maka diperlukannya perlindungan yang berkaitan dengan kepentingan negara, kelompok dan individu untuk mengelola, mengoperasikan dan mengendalikan atas cara yang tidak dapat dipercaya dan tanpa hambatan. Sehingga dalam hal ini baik data individu ataupun kelompok yang tergolong dalam akses non-publik merupakan bagian dari pelanggaran terhadap akses yang tidak sah dari bagian sistem elektronik dan data elektronik.

Pada Undang-Undang ITE juga mengenal gangguan terhadap data komputer *(Data Interference)* rumusan deliknya terdapat pada Pasal 48, berbunyi:

(1)Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (1) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp2.000.000.000,00 (dua miliar rupiah).
(2)Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (2) dipidana dengan pidana penjara paling lama 9 (sembilan) tahun dan/atau denda paling banyak Rp3.000.000.000,00 (tiga miliar rupiah).
(3)Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (3) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah).

Terkaitan unsur dalam Pasal 32 UU ITE berbunyi

(1)Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik.

(2)Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak.

(3)Terhadap perbuatan sebagaimana dimaksud pada ayat (1) yang mengakibatkan terbukanya suatu Informasi Elektronik dan/atau Dokumen Elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya.

Objek dari unsur Pasal 32 yang dimaksud ialah penghapusan data sebagai tindakan dilakukan atas memusnahkan terhadap data, yang bertujuan menghancurkan atau menyebabkan data komputer tidak lagi dikenal oleh program komputer yang dipakai oleh pemiliknya. Cara yang dilakukan dengan berupa menghalangi dengan segala cara mencegah dan menghentikan akses supaya data tersebut tidak dapat diakses. Disebutkan merubah berarti adanya modifikasi terhadap data yang ada. Sehingga gangguan terhadap data komputer diartikan merubah, menghapus atau menjadikan data tersebut tidak lagi dapat digunakan sebagaimana mestinya oleh pemilik data.

Melihat perkembangan modus kejahatan siber yang berkaitan dengan data pribadi ada beberapa serang siber terkait data pribadi atau penyimpanan terkait *database* yang terdapat informasi/data sensitf atau yang dianggap penting. *SQL Injection* atau sebuah bahasa untuk mengakses data dalam basis data relasional atau suatu sistem manajemen data, *SQL Injection* biasanya dilakukan pada aplikasi pengguna dengan cara memodifikasi perintah SQL, dengan tujuan mengekploitasi web aplikasi yang di dalamnya menggunakan databse untuk penyimpanan data, ini juga dianggap penyerangan terhadap data penyimpanan yang paling rawan diserang

pada sistem jaringan tanpa merusak keamanan sistem, sebab adanya celah yang sulit ditutup oleh sistem keamanan dari *database*. Menurut Badan Siber dan Sandi Negara (BSSN) melalui *Voluntary Vulnerability Dsiclosure Program (VVDP)* menyatakan pada 2019 rentan terhadap serangan *SQL Injection*, teknisnya dilakukan dengan memanfaatkan celah keamanan pada layer basisdata yang disebabkan data yang diinput oleh pengguna tidak dilakukan validasi dan dimuat pada baris perintah *query SQL*. Ini terjadi ketika aplikasi gagal untuk memvalidasi data atau membersihkan data yang tidak dapat dipercaya (seperti data dalam bidang formulir web). Pelaku dapat menggunakan perintah yang dibuat khusus untuk mengelabui aplikasi agar meminta database. Dampak dari kejahatan ini pelaku dapat melakukan pencurian informasi sensitive yang tersimpan di database.[109] Dalam hal ini penyerangan yang dilakukan tanpa merusak sistem keamanan pada komputer tetapi dengan melihat celah dari sistem komputer

Penggumpulan data yang popular dengan menggunakan *web scarping/crawling*, tujuan penggunaannya untuk mendapatkan informasi dari *website* secara otomatis tanpa harus menyalinnya secara manual, sehingga pencarian akan informasi tertentu dapat dikumpulkan pada web baru. Secara teknisnya *web scraping* digunakan untuk mendapatkan informasi yang terfokus pada data dengan cara mengambil dan

[109] Badan Siber dan Sandi Negara, *Mengenal SQL Injection dan Cara Mencegahnya,* dalam https://bssn.go.id/mengenal-sql-injection-dan-cara-mencegahnya/ diakses 30 April 2021.

diekstrasi dengan ukuran data yang bervariasi. Adapun langkah pada penggunaan *web scraping* sebagai berikut:[110]

1. Pembuatan program yang mempelajari dokumen HTML dari website yang akan diambil informasinya untuk fokus pada data/informasi yang akan diambil;
2. Teknik navigasi pada website yang akan diambil informasinya untuk ditirukan pada web scraper tersebut;
3. Setelah mendapatkan informasi yang dituju nanti aplikasi *web scraping* mengotomatisasi pengambilan informasi dari website tersebut;
4. Kemudian dari data tersebut akan disimpan pada database dan di ekstraksikan.

Jika melihat unsur pada ketentuan dalam Undang-Undang ITE terkait dengan akses illegal tidak dapat diterapkan dalam hal pengambilan data/informasi melalui *web scraping*, sebab data yang diambil tidak merusak sistem keamanan dan melanggar akan akses data secara illegal dengan menerobos masuk pada sistem keamanan tersebut. Teknis pengambilan dan pengumpulan datanya pun mengambil informasi yang dapat diakses oleh publik dengan terfokus pada varian data yang dituju yang mana data tersebut tidak adanya atau tanpa kode keamanan.

Terkait dengan gangguan data *(data interference)* pada Undang-Undang ITE lebih mengarah pada data adanya perbuatan merubah, menghapus, dan

[110] Dhita Deviacita, Helen Sasty, dan Hafiz Muahardi, *Implementasi Web Scraping untuk pengambilan data pada situs marketplace,* Jurnal Sistem dan Teknologi Informasi, Vol 7, No. 4 Oktober 2019, hlm 258.

menyembunyikan data tersebut agak sistem komputer tidak mengenalinya serta menjadikan keutuhan data tersebut tidak sebagaimana mestinya dan diketahui oleh publik tentu dalam hal ini berbeda bila melihat cara kerja dari *web scraping,* metode pengumpulan data yang diambilnya *(copy-paste)* tidak melakukan suatu perubahan akan data serta menghilangkan atau bahkan data tersebut tidak lagi dapat digunakan oleh pemiliknya. Sehingga ketentuan dalam Undang-Undang ITE terkait unsur-unsur *data interference* terpenuhi.

Jangkauan dari Undang-Undang ITE sebagai bentuk perlindungan terhadap informasi atau data yang bersifat elektronik hanya mencakup terkait keamanan sistem yang mana dilakukan dengan cara membobol sistem keamanan komputer sehingga dianggap sebagai perbuatan akses illegal dan gangguan data yang mengarah pada dampak dari terhambatnya atau tidak dapat diaksesnya informasi dan data yang telah dilakukan perubahan baik itu menambah, mengurangi yang tidak sesuai dengan yang sebenarnya. Hal ini menjadikan kurang optimalnya Undang-Undang ini dalam memberikan jaminan terhadap pelanggaran ataupun kejahatan-kejahatan yang muncul terhadap peraturan yang ada.

Melihat data pribadi yang bersifat privasi erat kaitannya dengan ruang personal dan teritorialitas, ruang personal diartikan ketika adanya intervensi dari orang lain yang hadir, dan tidak lagi sebagai ruang personal lagi, bahkan menjadi ruang interpersonal. Kebutuhan akan privasi dimana memberikan batasan interaksi dengan orang lain dengan menjaga akan hal personalitias seseorang. Sedangkan

territorialitas sendiri dipahami sebagai hubungan antara kepemilikan atau hak seseorang atau kelompok tertentu atas sebuah lingkup tertentu.

Disamping itu berkaitan dengan privasi diartikan sebagai tingkatan interaksi atau keterbukaan seseorang yang dikehendaki terhadap suatu kondisi atau situasi tertentu, yang mana subjektifitas terhadap privasi yang dirasa hanyalah dapat diketahui dan dikontrol dari orang tersebut.[111]

Banyak produk perundang-undangan khusus (di luar KUHP) juga tidak menyebutkan/menentukan kualifikasi atas hal tersebut sebagai "kejahatan" atau "pelanggaran", sehingga secara yuridis menimbulkan kendala dalam implemetasi aturan hukum yang tidak secara khusus diatur dalam Undang-Undang khusus di luar KUHP.[112] Sehingga penerapan atas kejahatan siber terkait data pribadi sulit diterapkan dan mengakibatkan jaminan akan kepastian hukum serta perlindungan akan hak sulit terwujud.

B. Kendala Pada Undang-Undang Informasi Dan Transaksi Elektronik Dalam Menanggulangi Tindak Pidana Kejahatan Siber Terkait Perlindungan Data Pribadi Di Indonesia

Kejadian yang membuka mata atas data pribadi yang menyangkut hak privasi ketika seorang anggota keamanan nasional Amerika Serikat Edward J. Snowden

[111] Helmy Prasetyo Yuwinanto, Kebijakan Informasi dan Privacy, Paper, hlm 3

[112] Barda Nawawi Arief, *Perkembangan Sistem Pemidanaan Di Indonesia,* cetakan ketiga, (Semarang; Pustaka Magister, 2015),hlm 29-30

membocorkan sekitar 200.000 dokumen yang diekspos secara luas yang menyatakan bahwa ada tindakan pengawasan dari pihak intelejen AS dan sekutu terhadap warga lokal maupun internasional atas privasi seseorang dengan menggunakan pemanfaatan teknologi. Begitu juga yang disampaikan oleh pendiri Whistle Blowing AS Julian Assange menggemukakan hal yang serupa. Upaya intervensi terhadap hak seseorang akan privasinya tentu menjadi pelanggaran yang serius di negara tersebut yang mana menjunjung kebebasan terhadap indvidu. Pelanggaran atas data pribadi baik dari pihak penyelenggara jasa telekomunikasi dan pemerintah tentu harus ada batasan yang jelas sehingga adanya jaminan kebebasan dan perlindungan atas hak privasi yang berkaitan dengan data pribadi.

Secara umum kejahatan konvensional bergeser seiring dengan perubahan jaman dan pemanfaatan teknologi yang berkembang sebagai model dan sarana kejahatan yang berkembang. Fenomena pelanggaran privasi yang berkiatan dengan data pribadi sedang menjadi atensi atas kemajuan teknologi yang pesat. Kemunculan berbagai kejahatan yang menempatkan di ruang (siber) yang berbeda mengakibatkan aturan terhadap tindak kejahatan di ruang lingkup yang berbeda menjadi terbatas terhadap regulasi yang ada, jangkauan peraturan dalam menerapkan suatu aturan pun tidak bisa secara optimal dilakukan sebagai upaya penegakan hukum. Ini disebabkan pengaturan mengenai hal tersebut belum secara spesifik diatur tersendiri atau aturan yang ada tidak bisa mengikuti perkembangan yang ada. Pelanggaran tersebut tidak hanya sebagai bentuk pencurian terhadap

benda material, tetapi juga melanggar atas prinsip hak atas kebebasan privasi bukan hanya hak atas kepemilikian.

Mewujudkan ketertiban dengan sarana salah satunya dengan instrumen hukum merupakan bagian dari upaya yang secara efektif dianggap dapat tercipta suatu ketertiban terhadap pelanggaran-pelanggaran yang terjadi maupun yang akan datang. Penggunaan sarana pemidanaan sebagai *ultimum remediun* dianggap menjadi jalan terakhir dalam penegakan hukum, seiring dengan hal itu juga dapat memberikan jaminan perlindungan hukum terhadap masyarakat untuk dilindungi atas hak-haknya.

Berdsarakan uraaian di atas ada beberapa faktor yang menjadi kendala pada Undang-Undnag ITE dalam menanggulangi kejahatan siber berkaitan perlindungan data pribadi yang akan dikelompokkan menjadi dua bagian yaitu secara yuridis dan non-yuridis, pertama faktor yang mempengaruhi secara yuridis, yakni:

1. Undang-Undang yang mengatur tentang data pribadi tidak memberikan klasfikasi yang jelas bila dilihat dari berbagai Undang-Undang yang ada.

   Beberapa ketentuan yang mengatur mengenai data/informasi yang bersifat personal tidak memberikan penjelasan yang utuh mengenai data pribadi, sebab tindak pidana siber terkait perlindungan data pribadi hanya memberikan perlindungan terhadap akses yang sah terhadap sistem keamanan sebagai perlindungan terhadap informasi/data yang boleh diakses. Disamping itu juga delik pada gangguan data *(data interference)* hanya dapat menjangkau terhadap data yang dilakukan perubahan baik ditambah ataupun dikurangi, dimusnahkan

atau dihilangkan, serta kebenaran data tersebut yang sudah tidak semestinya yang mengarah pada data/informasi tersebut tidak lagi dikenal oleh sistem komputer atau tidak dapat diakses oleh pemilik data tersebut..

2. Undang-Undang ITE kurang memberikan definisi yang kompherensif dan jelas mengenai klasifikasi data pribadi yang bersifat elektronik dalam Undang-Undang ITE

   Delik dalam Undang-Undang ITE tidak menjangkau akan perubahan perkembangan modus operandi terhadap pencurian data pribadi yang mana dengan tanpa merusak sistem keamanan pada komputer dan menjadikan data/ informasi tersebut tanpa adanya gangguan data yang terdapat dalam sistem komputer. Disisi lain penyidik dalam melakukan upaya penyidikan terhaambat akan penerapan ketentuan yang ada dalam Undang-Undang ITE.

3. Keterbatasan terhadap pelaku (subyek) pada Undang-Undang ITE berkaitan dengan illegal akses

   Unsur dari pelaku yang hanya dapat diterapkan terhadap pelaku yang tidak memiliki kewenangan akan akses atas data yang bersifat elektronik, artinya terhadap pelaku yang memiliki kewenangan (otoritasi) tetapi dalam hal ini menyalahgunakan kewenangan atau melampaui hal tersebut terhadap data pribadi yang bersifat elektronik untuk kepentingannya sulit untuk diterapkan terhadap Pasal 30 Undang-Undang ITE mengenai akses illegal.

Kedua, faktor yang menjadi kendala dalam penegakan hukum (non-yuridis), yakni:

1. Minimnya kesadaran masyarakat akan pentingnya perlindungan data pribadinya sendiri.

   Tolak ukuran akan identitas yang patut dilindungi oleh setiap orang di masyarakat masih berbeda-beda, sehingga menimbulkan perbedaan akan pemahaman standar akan data pribadi apa saja yang perlu dilindungi dan boleh diakses oleh publik di dunia virtual.
2. Sulitnya dalam mencari bukti telah terjadi pencurian data pribadi

   Pada umumnya pencurian data pribadi dalam hal ini sering kali pemilik tidak menyadari bahwa data pribadinya telah diambil dan diakses oleh pelaku tanpa adanya ijin dari pemilik data. Bahkan pemilik data baru mengetahui ketika adanya pemberitaan mengenai kebocoran data pribadi pada beberapa akun sosial media melalui pemberitaan.
3. Sulitnya bagi masyarakat yang tidak memiliki teknologi muthakir dalam mengetahui keamanan sistem teknologi.

   Keterbatasan terhadap pemahaman literasi digital dan perangkat digital modern yang dimiliki juga dianggap salah satu faktor di masyarakat akan minimnya upaya pencegahan akan kejahatan siber terkait data pribadinya.

Dari beberapa faktor yang diuraikan, tentu sangat berpengaruh terhadap penegakan hukum itu sendiri. Perlunya kesadaran masyarakat akan data pribadinya di ruang siber sangat rentan bila disalahgunakan atau adanya akses tanpa ijin dari pihak lain, dan perlunya juga pihak penyedia baik itu provider dan pemerintah yang menangani dalam hal pengawasan dan melindungi masyarakat yang awam akan hal

perlindungan data pribadi mereka, yang bertujuan agar dapat meminimalisir dan melindungi data pribadi masyarakat.

Beberapa kejadian yang pernah terjadi di Indonesia terkait dengan pencurian data pribadi salah satunya data pribadi yang disebarkan melalui media sosial yang mencantumkan nomor identitas penduduk (NIK), alamat bahkan nomor kartu keluarganya. Dugaannya bahwa data pribadi yang beredar pada media sosial merupakan data yang diberikan kepada salah satu provider telekomunikasi sebagai syarat aktifasi kartu. Berdasarkan penyidikan bahwa pelaku merupakan bagian dari pihak intern tetapi dalam hal ini tidak memiliki otoritas akan mengakses data tersebut baik dari pemilik data maupun pimpinan dari perusahaan tersebut. Lain hal kasus yang terjadi terhadap dua market place *(e-commerce)* ternama yaitu bukalapak dan tokopedia yang mana terjadi pembobolan data base server internal yang berimbas pada data base dari para pengguna market place tersebut. Hingga kini kasus tersebut sudah dilakukan investigasi oleh penegak hukum tetapi tidak juga memberikan gambaran yang jelas mengenai pelaku yang menjadi aktor pembobolan terhadap data base server internal tersebut. Melihat dari beberapa kejadian yang terjadi dalam hal ini bahwa penegak hukum dirasa kurang optimal dalam melakukan pengusutan atas kasus tertentu.

Kesadaran masyarakat akan data pribadi mereka terlihat dari kebijakan terbaru yang dikeluarkan oleh platform media sosial berbasis *chatting* tentang pengelolaan data pribadi yang dianggap berbeda dengan kebijakan terdahulu terkait dengan akses data pengguna, kebijakan tersebut juga dianggap oleh sebagian pengguna

terhadap data yang diminta dan diakses oleh pihak platform dianggap tidak sesuai dengan kewenangan platform untuk mengakses informasi baik data ataupun perilaku pengguna *(behavior of user)*, misalkan akses lokasi pengguna apabila oleh pengguna tidak diijinkan untuk mengakses tetapi pihak platform dapat mengakses dengan menggunakan alamat IP, jaringan seluler, IMEI, dan ISP. Sehingga menimbulkan penolakan oleh pengguna dari platform tersebut untuk beralih menggunakan yang lebih memberikan perlindungan akan data pribadinya, semata-mata agar terhindari dari penyalahgunaan atas data pribadi di ruang siber.

Ciri karakterisitik dari kejahatan siber berkaitan dengan data pribadi perlu juga dilihat mengenai upaya yang dianggap relevan dengan memberikan sanksi yang secara tepat dapat memberikan efek pembinaan dan edukasi, umumnya pelaku kejahatan siber memiliki keterampilan yang khusus dalam hal mengoperasikan komputer serta program pengaplikasiannya, terdidik, perangkat teknologi yang rumit dan kompleks menjadikan tantangan dalam mengulik sistem teknologi, kreatif dan ulet.[113] Kejahatan siber memiliki karakteristik yang berbeda dengan kejahatan di luar dari kejahatan siber, dapat dilihat dalam Undang-Undang ITE mengenai bentuk-bentuk yang telah diatur mengenai klasifikasi kejahatan siber, untuk kejahatan siber berkaitan dengan data pribadi menurut penulis serupa dalam hal bentuk dari kejahatan siber yang terjadi, tetapi perkembangan atas teknologi juga mempengaruhi akan perkembangan kejahatan di dunia siber.

[113] Besse Sugiswati, op. cit., hlm 66.

Menurut Barda Nawawi Arif mengenai upaya penegakan hukum pidana tidak mutlak pada lingkup tataran teknik perundang-undangan saja yang dilakukan secara yuridis normatif dan sistemik dogmatik. Perlu juga melakukan pendekatan diluar yuridis faktual seperti pendekatan sosiologis, historis, dan komperatif dan lebih luas lagi menggunakan pendekatan kompherensif dari berbagai disiplin ilmu sosial lainnya, serta pendekatan kebijakan sosial. Sehingga dapat memberikan gambaran yang menyeluruh dalam menentukan upaya penegakan hukum pidana yang efektif.[114]

Klasifikasi mengenai data pribadi yang ada pada berbagai undang-undang yang menyangkut atas data seseorang menjadikan setiap definisi dan makna akan data pribadi di setiap undang-undang berbeda antara satu dengan yang lain. Ini terjadi karena dalam pembentukan undang-undang sendiri memahami setiap data pribadi yang berkaitan dengan privasi seseorang berbeda-beda. Sehingga tidak ada kesatuan makna akan definsi yang definitif terhadap data pribadi yang dapat dijadikan acuan sebagai klasifikasi data pribadi elektronik, serta berdampak tidak adanya kepastian hukum mengenai perlindungan data pribadi. Pengaturan berkaitan dengan perlindungan data pribadi juga terletak pada berbagai undang-undang yang mengakibatkan tidak adanya harmonisasi dalam tataran normatifnya. Begitu juga terhadap Undang-Undang ITE yang mengatur tentang pemanfaatan teknologi

[114] Besse Sugiswati, op. cit., dikutip dalam bukunya Andi Hamzah, *Sistem Pidana dan Pemidanaan di Indonesia,* tanpa cetakan, (Pradnja Paramita: Jakarta, 1993), hlm 24.

sebagai salah sata sarana atas kemajuan teknologi sebagai penggunaan, pengumpulan, dan penyebaran terhadap data seseorang di ruang siber. Bila ditelaah mengenai definisi secara khusus juga tidak terdapat dalam Undang-Undang tersebut. Namun pengaturan sanksi terhadap pelanggaran atas data pribadi lebih kepada pelanggaran atas akses terhadap keamanan suatu sistem teknologi terhadap data yang ada di dalamnnya, baik dilakukan dengan mengubah, menghapus, mengelola, dan meng-input terhadap data di dalamnya. Akan tetapi terhadap data pribadi itu sendiri bila terjadi pelanggaran yang menimbulkan kerugian bagi pemilik data hanya dapat dilakukan gugatan kerugian secara perdata. Impikasi dampak dari data pribadi tidak dapat diukur dengan tolak ukur yang dapat diperhintungkan, apalagi terhadap hal tersebut dijadikan suatu yang untuk menghasilkan keuntungan bagi pihak tertentu baik secara finansial, politik dan lainnya. Hal ini tentu tidak terwujudnya akan hak asasi seseorang pada perlindungan atas data pribadinya sebagai pengguna dan pemilik data di ruang siber.

Klasifikasi berkaitan data pribadi yang patut diakses secara publik dan khusus pun tidak terdapat dalam Undang-Undang ITE, yang menjadikan secara patut data yang perlu dijaga dan dilindungi tidak bisa diakses di ruang publik atau diketahui oleh umum. Bila mengacu pada peraturan yang ada tentu akan terkendala mengenai data pribadi yang dilindungi, sebab setiap ketentuan mengenai data pribadi diatur secara sebagian menyesuaikan dengan muatan utama dari perundang-undangannya. Padahal pemilik data pribadi menjadi pemegang hak yang tentu nilanya berharga.

Yang mempengaruhinya adalah adanya hak asasi akan data seseorang baik identitas maupun yang menyangkut pada ruang privasinya tidak terlindungi, sehinggal hal tersebut tidak diperbolehkan bila menimbulkan kerugian baik oleh siapapun. Menurut *US dapartemen of Justice* yang mengelompokkan jenis-jenis *computer fraud* salah satunya termasuk pencurian identitas, skema yang sering dilakukan melibatkan pencurian identitas yaitu dengan memperoleh dan menggunakan data personal orang lain untuk melakukan *fraud* atau penipuan demi tujuan ekonomis, misalnya pelaku memperoleh data personal baik nama dan nomor *social security* sejumlah pejabata militer AS kemudian digunakan untuk memperbanyak dengan membuat aplikasi kartu kredit via internet pada *Delaware Bank.*[115]

Bila melihat dibeberapa negara-negara lain yang menurut penulis perlu dijadikan sebagai bahan untuk referensi dalam mengatur berkaitan dengan data pribadi yang mana memiliki regulasi mengenai perlindungan data pribadi, misalnya Filipina, yang secara resmi diundangankannya Undang-Undang No, 10173 (*Republic Act No. 10173)* tahun 2012 tentang Data Pribadi, sebelum peraturan ini muncul Filipina juga telah memilki peraturan yang berkaitan dengan keamanan data pribadi. Ketentuan pidana dalam undang-undang ini terdapat dalam BAB VIII, menjelaskan secara rinci denda atas pelanggaran undang-undang serta ancaman pidananya juga. Klasifikasi yang dianggap sebagai suatu pelanggararan terhadap data pribadi meliputi; pengelolaan yang tidak sah dari suatu informasi pribadi, akses yang tidak

[115] Abdul Wahid dan Mohammad Labib, op.,c it, hlm 81.

sah, penghancuran infromasi pribadi senyatanya tidak tepat, pelanggaran keamanan terhadap informasi sensitif dan pengungkapan informasi secara tidak sah. Berdasarkan undang-undang ini sanksi yang diberikan berupa denda antara lima ratus sampai dengan lima juta peso Filipina, serta ancaman pidana penjara paling sedikit satu tahun enam bulan atau selama-lamanya tujuh tahun. Penjatuhan pidana bila dilakukan oleh korporasi maka tanggung jawab pidananya diberikan kepada individu yang memiliki tanggungjawab dalam pengelolaan data/atau pihak yang turut serta memberi sponsor terjadinya pelanggaran tersebut. Tidak hanya pidana penjara yang dijatuhkan terhadap korporasi, pengadilan juga dapat mencabut ijin serta hak-hak yang dimiliki korporasi tersebut. Apabila warga negara asing yang menjadi pelakunya, maka sanksi hukum yang diberikan juga berupa deportasi setelah menjalani masa hukumannya.[116]

[116] Abdul Djafar, op., cit., hlm 14-15.

BAB IV

PENUTUP

A. Kesimpulan

Berdasarkan pembahasan yang telah dikemukakan pada bab-bab sebelumnya, maka penulis dapat mengambil dkesimpulkan sebagai berikut:

1. Kemampuan Hukum Pidana terhadap kejahatan siber terkait data pribadi dalam Undang-Undang Informasi dan Transaksi Elektronik dapat diterapkan mengenai Pasal tentang akses illegal, sebab data pribadi yang bersifat elektronik termasuk bagian dari informasi elektronik yang juga berupa sekumpulan data elektronik yang tidak terbatas pada tulisan, suara, gambar yang dilindungi atas kerahasiaannya dalam sistem elektronik. Pasal 30 Undang-Undang Informasi dan transaksi elektronik mengatur mengenai akses illegal yang terdapat adanya pembatasan terhadap akses dalam sistem elektronik, yang mana ciri dari pembatasan akan akses adanya suatu pengamanan baik dari kode akses atau *password* tertentu atau dengan menggunakan bahasa pemograman untuk masuk dengan membobol sistem kemananan, disamping itu untuk mengetahui bahwa data elektronik tersebut merupakan akses publik atau tidak dengan melihat adanya suatu sistem keamanan. Keterbatasan pada Undang-Undang ITE tidak dapat menjangkau akan modus yang dilakukan tanpa merusak sistem keamanan dan perubahan data yang dilakukan *(data interference)* baik itu menghilangkan

atau memnusnahkan data tersebut sehingga tidak lagi dapat dikenali oleh sistem komputer.

2. Upaya perlindungan data pribadi yang bersifat elektronik oleh penegak hukum hingga saat ini masih minim, lahirnya Undang-Undang informasi dan transaksi elektronik bertujuan untuk meminimalisir kejahatan baru dan perlindungan hukum yang dilakukan dengan sarana pemanfaatan teknologi pada sistem elektronik. Perlindungan atas data elektronik hanya sebatas pada adanya illegal akses dan gangguan data *(data interference)* dalam memberikan perlindungan terhadap sistem keamanan, tidak termasuk data yang bersifat khusus yang ada dalam sistem elektronik. Disamping itu menurut penulis dalam hal ini justru terkendala juga pada beberapa pasal yang kurang menjangkau dan tidak adanya aturan yang jelas atas perlindungan data pribadi pada Undang-Undang ITE. Padahal tujuan dari pembentukan Undang-Undang ITE untuk memberikan jaminan perlindungan atas informasi/data elektronik, kepastian hukum dan keadilan di masyarakat atas dampak perbuatan pelanggaran yang merugikan masyarakat.

B. Saran

Saran penulis adanya aturan yang memberikan gambaran secara kompherensif mengenai perlindungan data pribadi yang bersifat elektronik untuk memberikan perlindungan hukum serta perlu dilakukannya harmonisasi pada Undang-Undang yang berkaitan dengan pengaturan dan klasifikasi data/informasi pribadi.

DAFTAR PUSTAKA

Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (Cybercrime)*, Cetakan kedua (Bandung: Refika Aditama, 2010).

Afitrahim, *Yurisdiksi Dan Trasnfer of Proceeding Dalam Kasusu Cybercrime,* Tesis, Universitas Indonesia, 2012.

A. Cey Kurnia, *Penerapan Prinsip Yurisdiksi Universal Terhadap Penegakan Hukum Dalam Tindak Pidana Siber (Cybercrime) Di Indonesia*, Tesis, Magister Hukum, Program Pascasarjana, Universitas Padjajaran, tanpa tahun penerbitan.

Agus Raharjo, *Cybercrime: Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi,* cetakan pertama, (Citra Adhitya Bakti, Bandung, 2002).

Al. Wisnubroto, *Konsep Hukum Pidana Telematika*, cetakan pertama, (Yogyakarta: Universitas Atma Jaya, 2011).

Andi Hamzah, *Sistem Pidana dan Pemidanaan di Indonesia*, tanpa cetakan, (Pradnja Paramita: Jakarta, 1993).

Barda Nawawi Arief, *Beberapa Aspek Kebijakan Penegakan dan Pengembangan Hukum Pidana,* cetakan pertama, (Bandung: Citra Aditya Bakti, 1998).

_____, *Sari Kuliah: Perbandingan Hukum Pidana*, Cetakan I, (Jakarta: Raja Grafindo Persada, 2002).

_____, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan,* cetakan ketiga, (Kencana Prenada Group; Jakarta, 2010).

_____, *Kebijakan Hukum Pidana*¸ cetakan -----, (Bandung; Citra Aditya Bakti, 2002).

_____, *Kebijakan Legislatif Dalam Penanggulangan Kejahatan Dengan Pidana Penjara,* Cetakan keempat, (Yogyakarta: Genta Publishing, 2010).

_____, *Perkembangan Sistem Pemidanaan Di Indonesia,* cetakan ketiga, (Semarang; Pustaka Magister, 2015).

_____, *Bunga Rampai Kebijakan Hukum Pidana,* cetakan kelima, (Jakarta: Kencana, 2016).

Bambang Poernomo, *Hukum Pidana Kumpulan Ilmiah,* Cetakan pertama, (Jakarta: Bina Aksara, 1982).

Eddy O. S. Hiariej, *Prinsip-prinsip Hukum Pidana,* cetakan kelima, (Cahaya Atma Pustaka, Yogyakarta, 2016).

Edmon Makarim, *Tanggung Jawab Hukum Penyelenggara Sistem Elektronik,* (Jakarta: Raja Grafindo Persada, 2010).

H. Jhon Kenedi, *Kebijakan Hukum Pidana: Dalam Sistem Penegakkan Hukum Di Indonesia,* Cetakan Pertama, (Yogyakarta: Pustaka Pelajar, 2017).

Indariyanto Seno Adji, *Keorupsi dan Penegakan Hukum,* cetakan pertama, (Jakarta: Dadit Media, 2009).

Indraswari Rahajeng, *Yurisdiksi Kriminal Berlakunya Hukum Pidana Nasional Terhadap Cybercrime Di Luar Yurisdiksi Indonesia*, Tesis, Magister Hukum, Program Studi Magister Hukum, Universitas Andalas, 2017.

Jack Febrian, *Menggunakan Internet*, tanpa cetakan, (Bandung: Informatika, 2003).

J. Remmelink, *Pengantar Hukum Pidana Material; Prolegomena dan Uraian Tentang Teori-Ajaran Dasar,* Tristam P. Moeliono (penerjemah), (Yogyakarta: Maharsa, 2014).

Kementrian Pertahanan Indonesia, *Pedoman Pertahanan Siber*, tanpa cetakan, (Jakarta: Kemenhan RI, 2014).

Leden Marpaung, *Asas-Teori-Praktik Hukum Pidana,* cetakan ketujuh, (Jakarta: Sinar Grafika, 2012).

Muhammad Mustofa, *Kriminolagi Kajian Sosiolagi Terhadap Kriminalitas, Perilaku Menyimpang dan Pelanggaran Hukum,* (Depok: Fisip UI Press, 2007).

M. Hatta, *Kebijakan Politik Kriminal; Penegakkan Hukum Dalam Rangka Penanggulangan Kejahatan,* Cetakan pertama, (Yogyakarta: Pustaka Pelajar, 2010).

Muladi, *Kapita Selekta Sistem Peradilan Pidana,* (Semarang: Badan Penerbit Undip, 2004).

Mukkti Fajar dan Yulianto Achmad, *Dualisme Penelitian Normatif dan Empiris*, Cetakan pertama, (Yogyakarta: Pustaka Pelajar, 2009).

Moh. Hatta, *Beberapa Masalah Penegekan Hukum Pidana Umum dan Pidana Khusus,* Cetakan pertama (Yogyakarta; Liberty, 2009).

Moeljatno, *Azas-azas Hukum Pidana*, Cetakan keempat, (Jakarta: Bina Aksara, 1987).

Mardjono Reksodiputro, *Menyelaraskan Pembaruan Hukum,* cetakan pertama, (Jakarta: Komisi Hukum Nasional, 2009).

Puslitbang Hukum dan Peradilan, *Naskah Akademis Kejahatan Internet (cyber crimes),* Mahkamah Agung, 2004.

Peter Marzuki, *Penelitian Hukum,* tanpa cetakan, (Jakarta: Kencana, 2007).

Rusli Muhammad, *Sistem Peradilan Pidana Indonesia,* Cetakan pertama, (Yogyakarta; UII Press, 2011).

Roeslan Saleh, *Beberapa Asas Hukum Pidana Dalam Perspektif*, Tanpa Cetakan (Jakarta: Aksara Baru, 1983).

_____, *Segi Lain Hukum Pidana,* cetakan pertama, (Jakarta: Ghalia Indonesia, 1984).

Roeslan Saleh, *Beberapa Asas Hukum Pidana Dalam Perspektif,* Tanpa Cetakan, (Jakarta: Aksara Baru, 1983).

Satjipto Raharjo, *Masalah Penegakan Hukum; Suatu Tinjauan Sosiologis"*, tanpa cetakan, (Bandung: Sinar Baru, 1983).

Sinta Dewi Rosadi, *Cyber Law: Aspek Data Privasi Menurut Hukum Internasional, Regional, dan Nasional*, cetakan pertama, (Refika Aditama: Bandung, 2015).

Soerjono Soekanto, *Faktor-faktor Yang Memperngaruhi Penegakan Hukum*, edisi pertama, (Jakarta; Raja Grafindo Persada, 2007).

Sugeng, *Hukum Telematika Indonesia*, cetakan pertama, (Kencana; Jakarta, 2020).

Sudikno Mertokusumo, *Mengenal Hukum: Suatu Pnegatar*, cetakan lima, (Yogyakarta: Cahaya Atma Pustaka, 2003).

Sudaryono dan Natangsa Surbakti, *Hukum Pidana; Dasar-dasar Hukum Pidana Berdasarkan KUHP dan RUU KUHP*, tanpa cetakan, (Muhammadiyah University Press: Surakarta, 2017).

Teguh Prasetyo, *Kriminalisasi Dalam hukum Pidana*, cetakan pertama, (Bandung: Nusa Media, 2010).

Widodo, *Aspek Hukum Pidana Kejahatan Mayantara*, Cetakan pertama, (Yogyakarta: Aswaja, 2013).

Wahyudi Djafar dan Asep Komarudin, *Perlindungan Hak Atas Privasi Di Internet: Beberapa Penjelasan Kunci*, terbitan pertama, (Jakarta: ELSAM, 2014).

Wahyudi Djafar, Bernhard Ruben, dan Blandina, *Perlindungan data pribadi: Usulan Pelembagaan Kebijakan dari Perspektif Hak Asasi Manusia*, publis pertama, (Jakarta: Lembaga Studi dan Advokasi Masyarakat (ELSAM), 2016).

Wahyudi Djafar, *Perlindungan Hak Atas Privasi Di Internet, Beberapa Penjelasan Kunci*, publikasi pertama, (Jakarta: Lembaga Studi dan Advokasi Masyarakat (ELSAM, Jakarta, 2014).

Jurnal

Asa Intan Primanta, *Pertanggungjawaban Pidana pada Penyelahgunaan Data Pribadi*, Jurnal Jurist-Diction, Vol. 3, No. 4 Juli 2020.

Besse Sugiswati, *Aspek Hukum Pidana Telematika terhadap Kemajuan Teknologi di Era Informasi*, Jurnal Perpsektif, Vol. XVI, No. 1 Tahun 2011.

Dewa Gede Atmadja, *Asas-asas Hukum dalam Sistem Hukum,* Jurnal Kertha Wicaksana, Vol. 12, No. 2 2018.

Galuh Kartiko, *Pengaturan Tehradap Yurisdiksi Cyber Crime Ditinjau dari Hukum Internasional*, Jurnal Rechtldee edisi No. 2, Vol. 8 Desember 2013.

Iftah Putri Nurdiani, *Pencurian Identitas Digital Sebagai Bentuk Cyber Related Crime*, Jurnal Kriminologi Indonesia, Vol. 16, No. 2 November 2020.

Inue Rahmawati, *Analisis Manajemen Resiko Ancaman Kejahatan Siber,* Jurnal Pertahanan & Bela Negara, Vol. 7, No. 2 Agustus 2017.

Kusnu Goesniadhie, *Perpsektif Moral Penegakan Hukum yang Baik,* Jurnal Hukum, Vol. 17, No. 2 2017.

Mahrus Ali, *Proposional dalam Kebijakan Formulasi Sanksi Pidana,* Jurnal Hukum IUS QUIA IUSTUM, Vol 25, No. 1, 2018.

Marchelino Cristian N, *Penerapan Asas Kekhususan Sistematis sebagai Limitasi antara Hukum Pidana dan Hukum Pidana Administrasi,* Jurnal Hukum Unsrat edisi No.10, Vol. 23 desember 2018.

Muhamad Danuri dan Suharnawi, *Trens Cyber dan Teknologi Informasi di Indoensia,* Jurnal Infokam, Edisi XIII, No. 2 Septemeber 2017.

Riza Azmi. "Sejarah dan Konteks Terminologi Siber" *Majalah Cyber Defense Community,* edisi pertama tahun 2020.

Rosalinda Elsina Latumahina, *Aspek Hukum Perlindungan Data Pribadi di Dunia Maya,* Jurnal Gema Aktualita, Edisi No. 2, Vol. 3, Desember 2014.

Sugeng Brantas, *Defence Cyber dalam Konteks Pandangan Bangsa Indonesia tentang Perang dan Damai,* Jurnal Pertahanan Vol. 2, No. 2 2014.

Sinta Dewi, *Cybercrime Dalam Abad 21: Suatu Perspektif Menurut Hukum Internasional,* Jurnal MMH Edisi 40, No. 4 Oktober 2011.

Shraddha Kulhari, *Data Proctetion, Privacy, and Identity: A Complex Triad,* (Nomos Verlagsgesellschaft).

Sinta Dewi, *Prinsip-prinsip Perlindungan Data Pribadi di Nasabah Kartu Kredit Mneurut Ketentuan Nasional dan Implementasinya,* Jurnal Sosiohumaniora, Vol. 19, No. 3 2017.

Tim APJII, "Penetrasi dan Profil Perilaku Pengguna Internet Indoensia", *Buletin Asosiasi Penyelenggara Jasa internet Indonesia (APJII),* Edisi 40 Mei 2020.

Wahyudi Djafar, Seminar Online, *Perlindungan Data Pribadi dalam Pengelolaan Data Bantuan Sosial.*

Yasmirah Mandasari S dan Dudung Abdul, *Perlindungan Data Elektronik Dalam Formulasi Kebijakan Kriminal Di Era Globalisasi,* Jurnal Soumatera Law Review, Vol. 3, No. 2, 2020.

Perundang-undangan

Undang-Undang Nomor 39 Tahun 1999 Tentang Hak Asasi Manusia

Undang-Undang Nomor 14 Tahun 2008 Keterbukaan Informasi Publik.

Undang-Undang Nomor 36 Tahun 2009 Tentang Kesehatan.

Undang-Undang Nomor 30 Tahun 2014 Tentang Administrasi Pemerintahan.

dalam Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Dalam Undang-Undang Informasi dan Teknologi Eletktronik

Internet

https://andi.link/hootsuite-we-are-social-indonesian-digital-report-2020/. Akses pada tanggal 8 Oktober 2020

https://tekno.kompas.com/read/2020/05/05/19080067/kasus-kebocoran-data-di-indonesia-dan-nasib-uu-perlindungan-data-pribadi?page=all. Diakses pada tanggal 14 Desember 2020.